

ACCESS TO USAREUR INSTALLATIONS

1. In light of heightened awareness worldwide, USAREUR's Installation Access Control Program is ongoing. The Army Europe (AE) Regulation 190-16 , Installation Access Control of March 2005 (and its German translation AE 190-16 G) cover the policies and requirements to gain access onto U.S. installations in Europe. Following the policies of the regulation will better protect facilities and personnel, including you. We need your cooperation and support to make this important program a success.

2. In general this regulation requires:

- a. Documentation (and possibly screening) to acquire an installation pass.
- b. Limited sign-in capability and limited access roster use and duration.
- c. A reduction in the number of USAREUR wide installation passes.
- d. Firms and site managers to be more accountable for their personnel while on the installation.
- e. A U.S. Government "sponsor" to determine your need to access installation(s) and assist you with IACS processing. Your sponsor is the organization (requiring Activity) to which you are directly providing the supplies or services. Contracting Offices will **not** normally be sponsors for contractors/vendors.

3. The documentation and processing required will depend on your "person" category as defined in AE regulation 190-16.

4. Registration will be accomplished by location. To minimize ant disruption, it is very important that you discuss with your requiring activity (RA) what the IACS requirements will be for your company. Ideally, the requiring activity will accompany you to the local Installation Access Control Office (IACO). If you are uncertain as to which organization is your requiring activity, please contact the Contracting Office that issued your contract for assistance locating the requiring activity.

5. Partnering and communication among all those involved in the process – you, your requiring/ sponsoring activity, and contracting and security personnel – will ensure the success of the Installation Access Control Program.

22 March 2005

Military Police

Installation-Access Control

***This regulation supersedes AE Regulation 190-16, 19 October 2003.**

The English version of this regulation is the governing directive for all person categories except for personnel employed under the provisions of the CTA II.

For the CG, USAREUR/7A:

E. PEARSON
Colonel, GS
Deputy Chief of Staff

Official:



GARY C. MILLER
Regional Chief Information
Officer - Europe

Summary. This regulation prescribes policy and procedures for installation-access control to U.S. Forces installations. This regulation does not apply to restricted areas governed by other regulations (AR 190-13).

Summary of Change. This regulation has been updated to—

- Eliminate all references to commercial solicitors.
- Add Host-Nation Government Official and Gate Guard categories and corresponding requirements (paras 28 and 29).
- Prescribe AE Form 190-16B, Receipt for Confiscated ID Card; AE Form 190-16C, Record of Destruction; AE Form 190-16D, IACS Identi-Kid Permission Slip; and AE Form 190-16E, IACS Installation-Pass-Holder Consent Form.
- Add procedures for retrieving installation passes or DOD ID cards from individuals who no longer require installation access or who have unserviceable or expired installation passes or DOD ID cards.
- Allow access by a valid visitor installation-pass holder when accompanied by the requester and when the individual must temporarily exceed his or her access level.
- Add procedures for issuing installation passes to new civilian hires who are unable to receive their Common Access Card (CAC) because of the recent DOD lockdown on CAC issuance (para 9c).
- Clarify that identification CACs without privileges (typically issued in the United States for either civilians or contractors) do not include the social security number on the back but will be processed as DOD ID-card holders for the purpose of IACS registration.
- Add organizations to perform sponsoring-organization responsibilities when access to more than three area support groups (ASGs) is requested (para 15d(2)(a)).

- Clarify that for those person categories where the foreign national screening (FNS) is required, the FNS applies to non-U.S. citizens and U.S. citizens who have lived in Germany for more than 12 consecutive months before an Installation Pass may be issued.
- Update the definitions of the Visitor (Immediate Family Member Living in Europe), Visitor (Friend or Family Member Not Included in Category Above), and Official Guest categories (paras 23 through 25, respectively).
- Update information for the Official Guest category (para 25).
- Add that, if not qualified for the German *Polizeiliches Führungszeugnis* (based on less than 1 year of residency in Germany), a Police Good Conduct Certificate (PGCC)-equivalent is required from the previous country of residence and it must be translated into English.
- Add that some non-German contractors with Technical Expert status may not be able to obtain the PGCC (*Polizeiliches Führungszeugnis*).
- Clarify that if an individual has a current security clearance, a check of the Defense Clearance and Investigation Index (DCII) is unnecessary.
- Clarifies that AE Form 604-1B must be signed by the individual on which an FNS is being conducted.
- Add guidance to limit base support battalion (BSB) risk.
- Add that a Residence Permit is required if staying in Europe longer than 90 consecutive days.
- Add that applicants must submit a copy of the agreement (club membership, *in loco parentis* memorandum, AE Form 600-700A) justifying the need for installation access.
- Clarify that people in the Local National Employee category (para 13) hired before 3 October 1985 are exempt from supplying a military police (MP) check.
- Clarify that people in the Local National Employee category (para 13) who are transferring from one organization to another without a break in service retain their status and will not be required to provide either a new PGCC or a new MP check.
- Clarify that applicants will turn in the expiring or expired Installation Pass or AE Form 190-16B receipt for it (if access-control personnel confiscated an expired pass) before receiving a new Installation Pass.
- Clarify that issuing officials should coordinate with the appropriate S-2 or security manager to determine the FNS status if the reason for the extension request is a delay in the FNS results.
- Clarify that if FNS results are not returned after the first 90-day extension (180 days), permission to re-extend the Temporary Installation Pass may be granted only by the USAREUR Provost Marshal (PM).
- Add that all personnel conducting access control may confiscate DOD ID cards or Installation Passes using AE Form 190-16B.
- Require installation access control office (IACO) registrars to record the destruction of all installation passes on AE Form 190-16C annotate the final disposition of passes in the Installation Access Control System (IACS).
- Add that IACOs will receive ribbons in addition to installation-pass cardstock and laminate from the USAREUR PM and that IACOs will keep an adequate stock of ribbons, passes, and laminate at all times.
- Add that a copy of the background-check initiation and results will be included in a complete application packet in addition to the application (AE Form 190-16A), a copy of supporting documents, the original copy of the acknowledgement of responsibilities memorandum, the Print Summary Page from the IACS, and the signed Privacy Act statement (for U.S. citizens only).
- Provide registration procedures for Identi-Kid (para 39).
- Add that original access-roster requests may be sent electronically from a *.mil*, *.gov*, or *.org* e-mail address.

- Add definitions for *in loco parentis* and PGCC.
- Require that guard SOPs include procedures for responding to each type of message available on the IACS handheld personal digital assistant (PDA) or IACS gate workstation (for example, Archived, Person Not Registered).
- Provide clarification on DD Form 2(RES).
- Remove 1st Personnel Command (1st PERSCOM) as a valid sponsor for the Vendor person category and remove references to 1st PERSCOM as an issuer of vendor permits.
- Remove specific chapter references to USAREUR Regulation 600-700.
- Clarify that commanders have the authority to administer punishment for individuals found to be in violation of their sign-in privileges.
- Update emergency-vehicle and protective-services-vehicle access language.
- Establish a requirement for AE Form 190-16E (when approved) to be signed and included in completed application packets for filing.

Applicability. This regulation applies to personnel requiring access to U.S. Forces-controlled installations. The 22d ASG and 80th ASG may develop policy and procedures that meet or exceed the standards of this regulation to meet their unique needs.

Supplementation. Organizations will not supplement this regulation without USAREUR PM (AEAPM-O-SO) approval.

Forms. This regulation prescribes AE Form 190-16A, AE Form 190-16B, AE Form 190-16C, AE Form 190-16D, and AE Form 190-16E. AE and higher-level forms are available through the Army in Europe Publishing System (AEPUBS).

Records Management. Records created as a result of processes prescribed by this regulation must be identified, maintained, and disposed of according to AR 25-400-2. File numbers and descriptions are available on the Army Records Information Management System Web site at <https://www.arims.army.mil>.

NOTE: In connection with the collection, processing, and submission of data of local national employees in Germany, organizations of the U.S. Forces must adhere to the provisions of the U.S. Privacy Act; other than that, the U.S. Privacy Act, as U.S. national law, does not apply to local national employees in Germany.

Suggested Improvements. The proponent of this regulation is the USAREUR PM (AEAPM-O-SO, DSN 381-7224). Users may suggest improvements to this regulation by sending DA Form 2028 to the USAREUR PM (AEAPM-O-SO), Unit 29931, APO AE 09086-9931.

Distribution. A (AEPUBS).

CONTENTS

SECTION I GENERAL

1. Purpose
2. References
3. Explanation of Abbreviations and Terms
4. General
5. Responsibilities
6. Policy
7. Exceptions to Policy

SECTION II INSTALLATION ACCESS

8. Access Methods
9. DOD ID-Card-Holder Access to Installations
10. Installation Passes

SECTION III INSTALLATION ACCESS CONTROL SYSTEM

11. IACS Registration
12. DOD ID-Card Holder
13. Local National Employee
14. Contractor (Based in United States)
15. Contractor (Living in Host Nation)
16. Personal-Service Employee
17. Delivery Personnel (Recurring Deliveries or Similar Service Not Associated With a Government Contract)
18. Vendor
19. NATO Member
20. Host-Nation Military Member
21. Foreign Student (Marshall Center)
22. Member of Private Organization
23. Visitor (Immediate Family Member Living in Europe)
24. Visitor (Friend or Family Member Not Included in Category Above)
25. Official Guest
26. Department of State and American Embassy Personnel
27. Other
28. Host-Nation Government Official
29. Gate Guard

SECTION IV INSTALLATION PASS

30. Application Process
31. Application Procedures for Applicant With Temporary Installation Pass
32. Application Procedures for Renewal Pass
33. Application Procedures for Lost or Stolen Pass
34. Application Procedures for Extension of Temporary Pass
35. Unserviceable Pass

SECTION V INSTALLATION ACCESS CONTROL OFFICE

36. General
37. Registration Procedures for Installation-Pass Applicant
38. Registration Procedures for DOD ID-Card Holder
39. Registration Procedures for Identi-Kid
40. Processing Access Rosters

SECTION VI ACCESS PROCEDURES

41. Sign-In Procedures
42. Access Rosters
43. Emergency-Vehicle and Protective-Services-Vehicle Access
44. ACP Guards

Appendixes

- A. References
- B. Format for Designation of Sponsoring Official's Memorandum
- C. Sample AE Form 190-16A
- D. Height and Weight Conversion Charts
- E. Sample Installation-Pass-Holder Acknowledgment of Responsibilities

Figures

1. Sample Temporary USAREUR/USAFE Installation Pass and USAREUR/USAFE Installation Pass
2. Sample AE Form 190-16B
3. Privacy Act Statement

Glossary

SECTION I GENERAL

1. PURPOSE

This regulation—

- a. Prescribes policy, responsibilities, and procedures for granting access to U.S. Forces installations in the USAREUR area of responsibility (AOR).
- b. Provides registration procedures for the Installation Access Control System (IACS).
- c. Provides procedures for preparing and issuing installation passes.
- d. Must be used with the following regulations:
 - (1) AR 600-8-14.
 - (2) AE Regulation 190-13.
 - (3) AE Regulation 525-13.
 - (4) USAREUR Regulation 600-700.
 - (5) USAREUR Regulation 604-1.

2. REFERENCES

Appendix A lists references.

3. EXPLANATION OF ABBREVIATIONS AND TERMS

The glossary defines abbreviations and terms.

4. GENERAL

- a. This regulation prescribes installation-access-control policy and provides procedures for personnel verification. Information on the physical design of an access-control point (ACP) may be found in Technical Manual (TM) 5-853-2 or provided by the installation antiterrorism officer, the physical security officer, or IMA-E.
- b. AE Regulation 525-13 prescribes policy and procedures for physically searching individuals and vehicles.
- c. Installation-access control in the USAREUR AOR depends on the successful use of the IACS. The IACS—
 - (1) Minimizes access to installations by persons using forged, invalid, or unauthorized access documents.
 - (2) Includes a database on individual-access privileges.
 - (3) Allows for centralized control of access privileges (for example, commanders may withdraw a terminated employee's access authorization).
 - (4) Produces installation passes.
 - (5) Enables ACP guards (referred to as "guards" in this regulation) to scan barcoded DOD identification (ID) cards and installation passes to verify access authorization and privileges.
 - (6) Provides an automated historical record of personnel who have accessed U.S. Forces installations.
- d. Sponsoring organizations and officials are critical to the success of the Installation Access Control Program.
- e. Individual access privileges are risk-based and depend on an individual's category (paras 12 through 29).

5. RESPONSIBILITIES

a. The USAREUR G2 will—

- (1) Manage the Foreign National Screening Program (USAREUR Reg 604-1).
- (2) Provide an automated system to support the foreign national screening (FNS) process.

b. The Inspector General, USAREUR, will include sponsor responsibilities as an area of special interest when inspecting organizations that sponsor installation-pass holders.

c. The Provost Marshal (PM), USAREUR, will—

- (1) Provide staff supervision and direction for the Installation Access Control Program.
- (2) Be the proponent for installation-access-control policy and the IACS. This includes system fielding, testing, life-cycle replacement management, and operator training.
- (3) Be the approving authority for written requests for exceptions to policy.
- (4) Coordinate the access-authorization decision with the sponsoring organization for all installation-pass applications when the results of any background check indicate derogatory information and U.S. Forces-wide access is requested.
- (5) Conduct staff assistance visits to review IACS registration and installation-pass-issuing procedures.
- (6) Ensure all installation access control offices (IACOs) comply with regulatory requirements.
- (7) Provide oversight for the procurement and security of installation-pass cardstock.
- (8) Perform automated audits on IACS-user activity.
- (9) Coordinate with the 1st Personnel Command (1st PERSCOM) and area support groups (ASGs) to ensure that the IACS database accurately shows all barred individuals.

d. The Commander, 1st PERSCOM, will—

- (1) Ensure that recipients of AE Form 600-700A understand that the form is not an installation-access document and that they must obtain an installation pass according to this regulation to enter U.S. Forces-controlled installations.
- (2) Provide the central depository for U.S. Forces-wide bars to installations and develop procedures for providing timely updates to bar rosters so that the IACS remains current and accurate.

e. ASG commanders will—

- (1) Develop policy to ensure access to base support battalions (BSBs) is controlled according to this regulation. ASG and BSB installation-access-control policy must not circumvent this regulation. For example, ASG commanders will not develop policy that honors only installation passes issued by their ASG or one of their subordinate BSBs. The intent of the Installation Access Control Program is for authorized access documents to be accepted at all U.S. Forces installations regardless of where the access document was issued. This does not include situations in which the guard has reason to question the authenticity of the access document.
- (2) Incorporate installation-access-control policy into organization inspection programs.
- (3) Establish procedures for coordinating with sponsoring organizations to determine access authorization for an installation-pass applicant when the results of a background check include derogatory information. This may be delegated to the BSB when access is limited to a single BSB.

(4) When an applicant is requesting access to more than one ASG, send the results of the background check with derogatory information to the USAREUR PM (AEAPM-O-SO), Unit 29931, APO AE 09086-9931.

(5) Develop procedures to notify the USAREUR PM of bars originating from an ASG that are not U.S. Forces-wide bars.

(6) Fulfill sponsoring-organization responsibilities where this regulation designates the ASG as the sponsoring organization.

(7) Consult the USAREUR PM on access options when access methods authorized by paragraph 8a do not adequately support co-use agreements with the host nation.

f. In addition to the responsibilities in subparagraph e above, the 22d ASG and 80th ASG commanders will adapt the policy and procedures of this regulation to meet their unique host-nation laws as needed (for example, requirements for background checks, obtaining fingerprints, vehicle registration, residence and work permits). The adapted policy and procedures must—

(1) Meet or exceed the security standards and intent of this regulation whenever possible.

(2) Be coordinated with and approved by the USAREUR PM and the Judge Advocate (JA), USAREUR.

g. BSB commanders will—

(1) Establish policy and procedures to enforce the provisions of this regulation in their AORs. This includes but is not limited to the following requirements:

(a) Procedures for DOD ID-card holders to register in and withdraw from the IACS during in- and outprocessing at either their servicing IACO or central processing facility (CPF).

(b) Procedures for retrieving installation passes or DOD ID cards from individuals who no longer require installation access or who have unserviceable or expired installation passes or DOD ID cards. AE Form 190-16B (available at <https://www.aeaim.hqusareur.army.mil/library/for/index-aei.shtm>) will be provided to the installation pass or ID card owner when an installation pass or ID card is confiscated. Confiscated DOD ID cards may not be destroyed. They must be provided to the nearest DOD ID card issuance facility for proper disposition within 24 hours after they are confiscated.

(c) A policy for IACOs to develop standing operating procedures (SOPs) that support this regulation.

(d) A policy for ACPs to have special guard orders that meet the scope and intent of this regulation. As a minimum, these special guard orders must include the following:

1. Instructions for sign-in procedures, access rosters, emergency and protective-services vehicles, and processing nonregistered DOD ID-card holders.

2. Instructions for handling unique access requests not covered by this regulation.

3. Instructions for conducting manual checks of access documents if IACS operations are disrupted.

4. Procedures for responding to vehicle drivers who disregard guard instructions (for example, failure to stop for access verification).

5. Procedures for responding to each type of message available on the IACS handheld personal digital assistant (PDA) or IACS gate workstation (for example, Archived, Person Not Registered).

6. A picture sample of the USAREUR/USAFE Installation Pass, the Temporary USAREUR/USAFE Installation Pass, and each type of DOD ID card.

7. Contact rosters for key personnel.

8. Map of the installation.

9. Telephone numbers for key organizations on the installation being guarded.

10. Random antiterrorism measures and force protection condition (FPCON) guidance.

11. Use-of-force guidance.

(e) Provide a copy of the ACP policy to the responsible German works councils.

(2) Ensure only authorized users have access to the IACS. Authorized users will be designated in writing with their user-level (for example, registrar, super-registrar).

(3) Provide an IACS-generated report with the names of individuals who are barred from entry to U.S. Forces installations to hiring agencies in their AOR. This report must be provided at least quarterly and when requested.

(4) Ensure proper security procedures are in place to safeguard IACS equipment at IACOs, CPFs, and ACPs.

(5) Ensure all IACS hardware transferred to the BSB is dedicated to support the IACS.

(6) Fulfill sponsoring-organization responsibilities where this regulation designates the BSB as the sponsoring organization.

(7) Ensure the responsible German works council is notified of emergency-access procedures for local national (LN) employees in accordance with paragraph 43.

h. BSB and area support team (AST) provost marshal offices (PMOs) will—

(1) On notification of a lost or stolen DOD ID card or installation pass, immediately flag the record in the IACS to deregister the lost card or pass.

(2) Develop procedures to support military police (MP) background checks required for installation passes (30b(5)). Copies of MP background-check results must be sent to the sponsoring organization. When the results include derogatory information, copies must be sent to the sponsoring organization and the ASG. ASG policy for processing background checks that result in derogatory information must be followed.

i. Contracting offices awarding contracts for supplies to be delivered to or for work to be performed on U.S. Forces-controlled installations will—

(1) Ensure the contract includes requirements for background checks and residence and work permits for installation passes and access rosters according to this regulation.

(2) Include a contract provision to ensure that contractors return all installation passes to the issuing IACO when the contract is completed or when a contractor employee no longer requires access (for example, quits, is terminated).

(3) Develop procedures to ensure requiring activities (k below) include the following information on all purchase requests and commitments (PR&Cs), military interdepartmental purchase requests (MIPRs), and other requests for contracting support when the contract will result in contractors requiring access to U.S. Forces installations in the USAREUR AOR:

(a) The name of the requiring activity and the name and telephone number of the requiring activity's installation-access POC.

(b) The location of the applicable IACO and the name and telephone number of the IACO POC.

j. Section V explains IACO responsibilities.

k. Sponsoring organizations will ensure—

(1) Sponsored personnel have a legitimate requirement to enter the installation.

(2) An installation-pass application (AE Form 190-16A) is prepared for each installation-pass applicant. The application will identify the applicant's access requirements and justify these requirements as required by this regulation (for example, when sign-in privileges are requested).

(3) Background checks on individuals seeking an installation pass are completed. When any derogatory information is discovered, the sponsoring organization must coordinate with the host ASG (or USAREUR PM if USAREUR-wide access is requested) to determine if the derogatory information should warrant denial of the request. The USAREUR G2 must be notified if derogatory information results in the denial of access privileges.

(4) The applicant registers his or her privately owned vehicle (POV) according to the procedures in this regulation and AE Regulation 190-1 (when applicable). Vehicle registration is required for all installation-pass applicants who use a POV to enter U.S. Forces installations. Contractor company vehicles are not considered POVs for the purpose of this regulation.

(5) The following information is included on all PR&Cs, MIPRs, and other requests for contracting support when the contract will result in contractors requiring access to U.S. Forces installations in the USAREUR AOR:

(a) The name of the sponsoring organization and the name and telephone number of its installation-access POC.

(b) The location of the applicable IACO and the name and telephone number of the IACO POC.

NOTE: If contractor access is not required, instead of providing the information in (a) and (b) above, sponsoring organizations may include the statement "This contract will not result in a contractor requiring access to a U.S. Forces installation."

(6) Contracting officers outside the purview of United States Army Contracting Command, Europe, are informed of installation-access policy in this regulation.

(7) Issued installation passes are retrieved and returned to the issuing IACO when the relationship that served as the justification for the installation pass changes or is terminated.

(8) A record of personnel sponsored by the organization and supporting documentation is maintained.

(9) A reconciliation with the servicing IACO is conducted every 6 months so that the IACS database accurately identifies individuals sponsored by the organization.

(10) A memorandum that designates persons authorized to perform sponsoring-official duties on behalf of the sponsoring organization (app B) is sent to the servicing IACO.

(11) Procedures in paragraph 30c are followed when the sponsoring official cannot escort the applicant to the servicing IACO.

1. Persons requiring recurring and unescorted access to U.S. Forces installations using a DOD ID card or installation pass will—

(1) Consent to the procedures for digitized fingerprint minutia data (DFMD) when—

(a) Inprocessing. Persons with an authorized, machine-produced DOD ID card will provide DFMD while inprocessing at their servicing IACO or CPF. If a DOD ID-card holder has a manually produced DOD ID card, that individual must obtain a machine-produced, barcoded DOD ID card according to the appropriate military regulations and personnel systems.

(b) Requesting an installation pass. Persons who do not have an authorized DOD ID card and require recurring unescorted access to U.S. Forces-controlled installations in the USAREUR AOR must request an installation pass. The installation pass will be issued only after the proper documentation has been submitted to the servicing IACO and the individual's DFMD has been provided.

(2) Carry their DOD ID card or installation pass on their person while in a duty status or when on a U.S. Forces installation. On request, they will present their DOD ID card or installation pass to military law-enforcement personnel or guards. Refusal to present their DOD ID card or installation pass is basis for the immediate surrender of the card or pass and may be grounds for further administrative or punitive action.

(3) Immediately report a lost or stolen DOD ID card or installation pass to the local MP office or servicing IACO so that the card can be deregistered.

(4) Inform the sponsoring organization of any change to the official relationship that served as the basis for access.

(5) Turn in the installation pass to the servicing IACO or sponsoring organization when the pass expires or when the basis for obtaining the installation pass no longer exists.

(6) Register his or her POV as part of the installation-pass-application process if planning to use the POV to enter U.S. Forces-controlled installations. Contractor company vehicles are not considered POVs for the purpose of this regulation.

m. Paragraph 44 prescribes ACP guard responsibilities.

6. POLICY

a. Commanders are responsible for the security of their installations and for ensuring the requirements of this regulation are enforced. Inconvenience to individuals is not a reason to circumvent or modify the procedures established by this regulation. These procedures will help—

(1) Support FPCON measures related to installation-access control.

(2) Identify barred individuals at U.S. Forces-installation ACPs.

(3) Prevent wrongful possession and pilferage of Government property and unlawfully bringing weapons, explosives, and other contraband onto U.S. Forces installations.

b. DFMD policy is as follows:

(1) Inprocessing. Personnel who possess an authorized DOD ID card and installation-pass applicants will provide DFMD during the IACS registration process.

(2) Identity Verification. Security or appropriate command personnel may require an individual to provide his or her DFMD for identity verification. This verification may routinely occur at ACPs to U.S. Forces installations. It may also occur at ACPs beyond the initial ACP. Refusal to provide DFMD may be the basis for immediate surrender of the individual's installation pass or DOD ID card and grounds for further administrative or punitive action by the command.

(a) Coordination must be made with host-nation police if the apprehension or search involves an LN citizen. If it involves an LN employee, the appropriate works council will also be consulted during official duty hours. If an LN employee is being apprehended or searched outside official duty hours, the appropriate works council will be informed immediately on the next workday.

(b) The installation-access policy is based on verifying the access authorization of every individual entering a controlled U.S. Forces installation, not vehicles or other means of transportation used to gain access. All individuals in vehicles or other modes of transportation will have their access-authorization verified according to the policy and procedures in this regulation.

(3) Identity Verification Other Than Authentication. If the request for the DFMD extends beyond identifying an individual, "probable cause" or other legal basis must be present before any apprehension or search. Coordination must be made with the servicing staff judge advocate office (when practical) if the request for the DFMD leads to an apprehension or search.

NOTE: The policy in subparagraph (3) above applies only to U.S. citizens.

7. EXCEPTIONS TO POLICY

a. Persons requesting an exception to any policy in this regulation must send their request through appropriate command channels to the USAREUR PM (AEAPM-O-SO), Unit 29931, APO AE 09086-9931, or by e-mail to iacs@manupo.pmo.army.mil.

b. Exceptions to policy approved after this regulation takes affect may be authorized and approved by the USAREUR PM for up to 1 year. Only the USAREUR PM may provide an exception to policy for a longer period and will do so only in writing.

c. Exceptions to policy that are imbedded in the IACS software application may be administered locally and do not require USAREUR PM approval.

d. Exceptions to policy outlined in paragraph 8b are not subject to this paragraph.

SECTION II INSTALLATION ACCESS

8. ACCESS METHODS

a. Personnel may obtain authorized access to U.S. Forces installations in the USAREUR AOR by one of the following four methods:

(1) Have a valid DOD ID card and be registered in the IACS (unless the exception to registration requirements in para 44e applies).

(2) Have a USAREUR/USAFE Installation Pass or a Temporary USAREUR/USAFE Installation Pass.

NOTE: A valid installation pass with TDY orders will authorize access when an individual must temporarily exceed his or her access level for operational reasons. A valid visitor installation-pass holder, when accompanied by the requester, will be authorized access when the individual must temporarily exceed his or her access level. The following are examples of when an increased level of access may be temporarily authorized:

Example 1: If an installation-pass holder has a 6th ASG-wide installation pass but must attend training in the 26th ASG AOR, his or her installation pass with TDY orders stating the training location and dates will be used to allow access. Because not all of these situations involve the issuance of TDY orders, other documents that state the purpose of travel and the location and dates are acceptable.

Example 2: If a visitor installation-pass holder has a 293d BSB-wide installation pass but accompanies the requester to an installation in the 415th BSB during the course of the visit, the visitor will be allowed access to the installation without being required to sign-in.

(3) Be signed in by an individual with sign-in privileges.

(4) Be on an approved access roster and present one of the documents listed in paragraph 30d(1).

b. The methods in subparagraph a above should be used with the policy and procedures in this regulation whenever possible. There may be situations, however, when commanders must supplement those methods for operational reasons (for example, large-scale training exercises that involve non-U.S. military members, running formations during organized unit physical training, military convoys). Exceptions to subparagraph a above must be explained in BSB policy and approved by the ASG commander. This subparagraph does not negate the policy in paragraph 7.

c. Paragraph 43 explains access policy for emergency and protective-services vehicles.

d. Memorandums, travel orders, AE Form 600-700A, a U.S. passport, NATO Sending State (Belgian, British, Canadian, Dutch, and French) ID cards, and DD Form 1172 are not access-authorization documents. Guards will not grant access based only on these documents. Individuals with these types of documents must be signed in by someone with sign-in privileges. All persons who used to obtain recurring, unescorted access using one of these or other types of documents must obtain an installation pass using the appropriate person category (paras 12 through 29).

e. Installation commanders will not further restrict access unless a bona fide need exists (for example, the installation has critical assets or restricted areas and there are no other layers of protection available). In these situations, commanders may determine that additional documents (such as a special pass) are required to gain access to their installation. Commanders are not authorized, however, to use these alternative access documents in place of DOD ID cards, USAREUR/USAFE Installation Passes, or Temporary USAREUR/USAFE Installation Passes.

f. Although a U.S. passport is not a valid access document, guards will not deny access to U.S. citizens who are not DOD ID-card or installation-pass holders during an emergency (for example, when the FPCON changes to Delta). Under these conditions, guards immediately will contact the MP office for assistance. An MP official will meet the U.S. citizen at the ACP and provide the necessary assistance for access.

9. DOD ID-CARD-HOLDER ACCESS TO INSTALLATIONS

a. A DOD ID card does not automatically authorize the cardholder access to U.S. Forces installations in the USAREUR AOR. The DOD ID card must have a readable barcode and the DOD ID-card holder must be registered in the IACS, unless the exception to the registration requirement in paragraph 44e applies. Personnel with a manually produced DOD ID card must obtain a machine-produced DOD ID card with a barcode according to the procedures established by appropriate military regulations and personnel systems.

b. The following machine-produced DOD ID cards (AR 600-8-14) are considered valid access documents:

(1) DD Form 2(ACT). This green card is issued to active duty military personnel. This card is being replaced by the Common Access Card (CAC) ((9) below).

(2) DD Form 2(RET). This blue card is issued to military retirees.

(3) DD Form 2(RES). This green card is issued to Reserve or National Guard personnel. This card is being replaced by the CAC.

(4) DD Form 2(RES RET). This red card is issued to Reserve and National Guard retirees.

(5) DD Form 1173. This tan card is issued to eligible military and DOD civilian-employee family members.

(6) DD Form 1173-1. This red card is issued to eligible Reserve and National Guard military and their family members.

(7) DD Form 1934. This card is issued to medical, religious, and auxiliary medical personnel who serve in or accompany the U.S. Armed Forces in combat regions and who may become prisoners of war.

(8) DD Form 2765. This tan card is issued to Medal of Honor recipients and honorably discharged veterans rated by the VA as 200-percent disabled from a uniformed service-connected injury or disease (other than current or retired members of the uniformed services).

(9) CAC.

c. The following applies to the civilian-hires DOD lockdown on CAC issuance:

(1) Definition. As a result of the DOD lockdown on issuing CACs to certain civilian hires, IACOs will issue a Temporary Installation Pass to qualified, affected civilian hires who are unable to receive their CAC when hired but who require access to USAREUR or USAFE installations.

NOTE: This affects only new civilian hires (new to the civilian system) and civilian employee transfers from one DOD organization to another (for example, Air Force to Army). It does not apply to same-service transfers of civilian personnel already in the system.

(2) Type of Pass Authorized.

(a) Temporary Installation Pass. People in this category may be issued a Temporary Installation Pass.

(b) Installation Pass. This pass is not authorized.

(3) Length of Time Pass Is Valid. The Temporary Installation Pass will be valid for a maximum of 90 days.

(4) Sponsor Requirements. The civilian personnel advisory center (CPAC) will perform sponsoring organization responsibilities for people in this category.

(5) **Background Checks.** Background checks are not required for people in this category.

(6) **Residence and Work Permits.** People in this category are not required to have residence or work permits.

(7) **Restrictions on Number of Installations a Pass Holder May Enter.** There are no restrictions on the number of installations. Outside the continental United States (OCONUS) civilian hires automatically receive access to U.S. Forces installations. No justification is required.

(8) **Restrictions on Days and Times Access Is Authorized.** There are no restrictions on when people in this category may access installations.

(9) **Restrictions on Sign-In Privileges.** People in this category will be limited to signing in four people and their vehicles.

(10) **FPCON Restrictions.** No FPCON restrictions apply.

NOTE: All CACs are made from white plastic card stock with no identifying color markings. CACs with a green stripe are issued to U.S.-citizen DOD contractors, who will be processed as DOD ID-card holders for the purpose of IACS registration. Identification CACs without privileges (typically issued to overseas family-member hires or in the United States to civilians or contractors) do not include the social security number on the back but will be processed as DOD ID-card holders for the purpose of IACS registration. CACs with a red vertical stripe on the right side of the card will not be recognized as an authorized access document. The red-striped CAC is issued to LN employees. LN employees must obtain an installation pass for access according to paragraph 13.

10. INSTALLATION PASSES

a. The two types of installation passes are the USAREUR/USAFE Installation Pass and the Temporary USAREUR/USAFE Installation Pass, which are referred to as “Installation Pass” and “Temporary Installation Pass,” respectively.

b. Temporary Installation Passes have a red background in the title block to distinguish them from the Installation Pass, which has a green background. Figure 1 shows samples of both passes. Although these installation passes are similar in appearance, the restrictions associated with each pass are different.

c. IACOs will not alter the appearance of installation passes with ASG- or BSB-unique features (for example, custom stamps, stickers, holograms).

d. The differences between the Temporary Installation Pass and Installation Pass include the following:

(1) A Temporary Installation Pass is valid for up to 90 days.

(2) If an Installation Pass is desired, a Temporary Installation Pass may be issued pending completion of a required background check. This balances security concerns with operational requirements. The use of successive Temporary Installation Passes is unauthorized, unless the exception in paragraph 34 applies.

e. Paragraph 11 provides requirements for registering installation-pass applicants into the IACS. The application procedures in paragraphs 12 through 29 must be completed before IACS registration may begin.

SECTION III INSTALLATION ACCESS CONTROL SYSTEM

11. IACS REGISTRATION

a. All DOD ID-card holders assigned in the USAREUR AOR and installation-pass applicants must be registered in the IACS. DOD ID-card holders who are on TDY orders to or visiting the USAREUR AOR may also be registered, depending on the length of their stay. For example, an individual with TDY orders to Germany for 2 days may not need to be registered, but an individual who will be on TDY in Germany for 1 month should be registered.

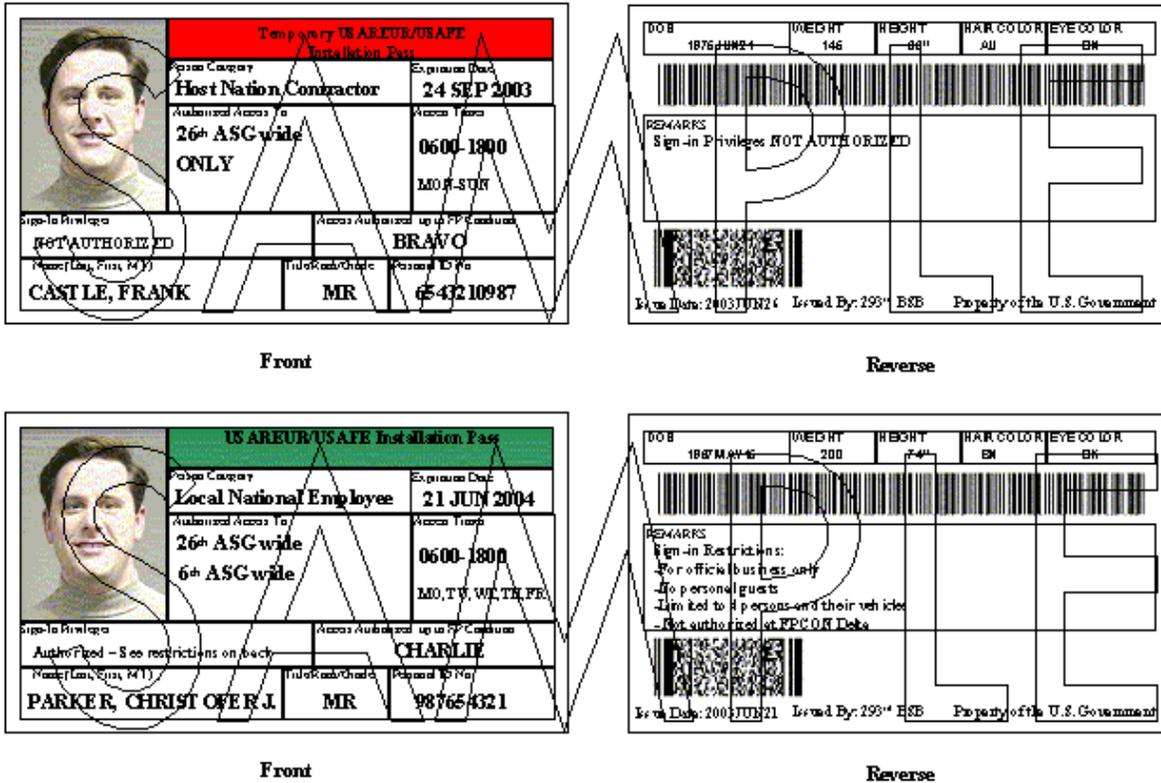


Figure 1. Sample Temporary USAREUR/USAFE Installation Pass and USAREUR/USAFE Installation Pass

b. Access by a nonregistered DOD ID-card holder will be recorded in the IACS. This procedure may cause nonregistered DOD ID-card holders a minor delay each time they enter an installation. The IACS also will track excessive numbers of times nonregistered DOD ID-card holders enter an installation. This will help identify possible unauthorized DOD ID-card holders (para 44e).

c. Section IV provides application procedures for installation passes.

d. An individual may qualify for one of the following categories:

- (1) DOD ID-Card Holder.
- (2) Local National Employee.
- (3) Contractor (Based in United States).
- (4) Contractor (Living in Host Nation).
- (5) Personal-Service Employee.
- (6) Delivery Personnel (Recurring Deliveries or Similar Service Not Associated With a Government Contract).
- (7) Vendor.
- (8) NATO Member.
- (9) Host-Nation Military Member.

- (10) Foreign Student (Marshall Center).
- (11) Member of Private Organization.
- (12) Visitor (Immediate Family Member Living in Europe).
- (13) Visitor (Friend or Family Member Not Included in Category Above).
- (14) Official Guest.
- (15) Department of State and American Embassy Personnel.
- (16) Other.
- (17) Host-Nation Government Official.
- (18) Gate Guard.

e. A dual-category individual (for example, a military retiree who is also a contractor) will be registered in the category that provides the greatest access privileges. The Official Guest (d(14) above) and Other (d(16) above) categories will never be used as a dual-category qualifier.

f. The categories in subparagraph d above are risk-based. Paragraphs 12 through 29 provide specific requirements for registration and access restrictions for each category.

12. DOD ID-CARD HOLDER

a. Definition. An individual authorized to possess a DOD ID card, including children under the age of 18. The status of a DOD ID-card holder will supersede other person categories (paras 11d(2) through (18)). For example, an LN employee married to a servicemember and entitled to DD Form 1173 will be treated as a DOD ID-card holder for the purpose of this regulation and will not be issued an installation pass or be required to be sponsored.

b. Type of Pass Authorized. Individuals possessing an authorized DOD ID card will obtain their ID card through procedures established by appropriate military regulations and personnel systems. These individuals must register at their servicing IACO or CPF during community inprocessing to be registered in the IACS but will not be issued an installation pass. If the DOD ID-card holder has a manually produced DOD ID card, that person must obtain a machine-produced (barcoded) DOD ID card. Individuals who have multiple DOD ID cards (for example, a military retiree who is now a DA civilian employee) must choose which DOD ID card they want to use for IACS registration and use this card to access the installation.

c. Length of Time Registration Is Valid. Registration is valid until the expiration date of the DOD ID card. In no case will the registration period exceed 5 years. For individuals who are in the USAREUR AOR temporarily (for example, on TDY), the registration period will be based on their established departure date.

NOTE: Because the IACS initially established an expiration date of registration based on DEROS, it is critical for anyone who registered before this change and who has been granted an extension (for example, a soldier with an approved foreign-service tour extension) to visit their servicing IACO or CPF to update the expiration date in the IACS.

d. Sponsor Requirements. Unlike people in other categories, DOD ID-card holders may sponsor themselves and do not need to submit an installation-pass application (AE Form 190-16A). DOD ID-card holders will provide the IACO or CPF the documentation that supports the requirement to be registered in the IACS. This documentation will also be used to determine the expiration date for many individuals. Examples of acceptable documentation include, but are not limited to, permanent change of station (PCS) and TDY orders, DA Form 31, SF 50-B, and DA Form 3434. The purpose of this documentation is to prevent individuals who illegally possess a DOD ID card from being registered in the IACS. Minors will be registered in the presence of a parent or legal guardian.

e. Background Checks. Background checks are not required for DOD ID-card holders.

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

g. Restrictions on Number of Installations a DOD ID-Card Holder May Enter. No restrictions apply unless imposed by an authorized commander.

h. Restrictions on Days and Times Access Is Authorized. No restrictions apply unless imposed by an authorized commander.

i. Restrictions on Sign-In Privileges. The DOD ID-card holder must be at least 18 years old, except for active duty military members. This privilege is limited to signing in four persons and their vehicles. No other restrictions apply unless imposed by an authorized commander.

NOTE: Commanders may restrict or withdraw individual access or privileges depending on the circumstances after consulting with the servicing staff judge advocate and IACO.

j. FPCON Restrictions. No restrictions apply.

13. LOCAL NATIONAL EMPLOYEE

a. Definition. An individual who is employed by DOD in the USAREUR AOR and is not entitled to one of the DOD ID cards listed in paragraph 9b. This category is primarily for host-nation employees in the USAREUR AOR.

NOTE: LN employees may be issued a CAC as DOD transitions to the requirement for all DOD-computer users to use a CAC to log onto Government computers. CACs issued to LN employees will have a red vertical stripe down the right side of the CAC. These CACs will not be used as installation-access documents.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass may be authorized after all required background checks have been completed and an FNS has been initiated. The Temporary Installation Pass will be used only until an Installation Pass is authorized.

(2) Installation Pass. This pass may be authorized after all background checks (including an FNS) have been completed and returned negative, with no entries.

NOTE: Background checks that uncover entries must be forwarded to the host ASG for adjudication. ASG, BSB, and other commanders and security personnel will strictly control security checks and treat them as confidential. Responsible commanders will ensure that only persons with a need to know have access to individual security files (AR 381-45). Background checks with entries will be passed through security channels to the local U.S. commander of the employee for action. Paragraph 30b(5)(b) has additional guidance.

c. Length of Time Pass Is Valid. A Temporary Installation Pass is valid for up to 90 days. An Installation Pass is valid for up to 5 years or until the expiration date of the supporting document (for example, passport) that was used to obtain the Installation Pass, whichever is earlier.

d. Sponsor Requirements. The organization that the LN employee will work for will perform the sponsor responsibilities in this regulation.

e. Background Checks.

(1) Police Good Conduct Certificate (PGCC) (*Polizeiliches Führungszeugnis*). This certificate is required before a Temporary Installation Pass may be issued.

(2) MP Check. This check is required before a Temporary Installation Pass may be issued. (**NOTE:** This applies only to U.S. citizens.)

(3) Defense Clearance and Investigation Index (DCII). If the applicant claims a previous affiliation with the U.S. Armed Forces and has a social security number, this check is required before a Temporary Installation Pass may be issued.

(4) FNS. This screening applies to both non-U.S. citizens and U.S. citizens who have lived in Germany for more than 12 consecutive months. This screening must be initiated before a Temporary Installation Pass is issued; it must be completed and returned negative, with no entries, before an Installation Pass is issued. Employees hired before 3 October 1985 are exempt from this requirement (USAREUR Reg 604-1).

f. Residence and Work Permits. These permits may be required if the applicant is not a European Union (EU) resident.

g. Restrictions on the Number of Installations a Pass Holder May Enter. The number of installations a pass holder may enter will be limited to the minimum required for the LN employee to perform his or her duties.

h. Restrictions on Days and Times Access Is Authorized. No restrictions apply unless specified by the sponsor.

i. Restrictions on Sign-In Privileges. Temporary Pass holders are not authorized sign-in privileges. Installation Pass holders are not authorized sign-in privileges unless sign-in privileges are justified by the sponsoring organization. If sign-in privileges are justified by the sponsoring organization, the Installation Pass holder may sign in up to four individuals and their vehicles “for official business only.” Sign-in privileges for Installation Pass holders are not authorized during FPCON Delta.

j. FPCON Restrictions. No FPCON restrictions apply.

14. CONTRACTOR (BASED IN UNITED STATES)

a. Definition. A person who lives in the United States and is contracted to work for DOD in the USAREUR AOR, but is not a DOD ID-card holder. Although this person category is authorized an Installation Pass, the pass is specially designed for contractors from the United States, but working in the USAREUR AOR temporarily.

NOTE: A person must be contracted to work for DOD to obtain an installation pass. Contractors who are only attempting to establish a contract with DOD will obtain access to U.S. Forces installations in the USAREUR AOR by an individual with sign-in privileges or through access-roster procedures.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass may be authorized for visits up to 90 days.

(2) Installation Pass. This pass may be authorized only if the person will be in the USAREUR AOR longer than 90 consecutive days.

c. Length of Time Pass Is Valid. The Temporary Installation Pass is valid for the length of the visit or up to 90 days, whichever is less. The Installation Pass is valid for the length of the visit (must be more than 90 consecutive days), up to 1 year, or until the expiration date of the supporting document (for example, passport) that was used to obtain the Installation Pass, whichever is earliest.

d. Sponsor Requirements. The organization inviting the contractor to or escorting the contractor in the USAREUR AOR will perform the sponsor responsibilities in this regulation.

e. Background Checks. No background checks are required for persons in this category.

f. Residence and Work Permits. A residence permit may be required (para 30b(6)).

g. Restrictions on Number of Installations a Pass Holder May Enter. The number of installations will be limited to the minimum required for the contractor to perform his or her duties.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions unless specified by the sponsor.

i. Restrictions on Sign-In Privileges. People in this category are not authorized to sign in guests.

j. FPCON Restrictions. No FPCON restrictions apply.

15. CONTRACTOR (LIVING IN HOST NATION)

a. Definition. A contractor who lives in the host nation, is contracted to work for DOD in the USAREUR AOR, and is not a DOD ID-card holder.

NOTE: A contractor must be contracted to work for DOD to obtain an installation pass. Contractors who are only attempting to establish a contract with DOD may be granted access only through an individual who has sign-in privileges or through access-roster procedures.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass may be authorized only after all required background checks are completed and an FNS has been initiated.

(2) Installation Pass. This pass may be authorized after all background checks (including an FNS) have been completed and returned negative, with no entries.

NOTE: Background checks that uncover entries must be forwarded to the host ASG for adjudication. ASG, BSB, and other commanders and security personnel will strictly control security checks and treat them as confidential. Responsible commanders will ensure that only persons with a need to know have access to individual security files (AR 381-45). Background checks with entries will be passed through security channels to the local U.S. commander of the employee for action. Paragraph 30b(5)(b) has additional guidance.

c. Length of Time Pass Is Valid. A Temporary Installation Pass will be valid for the length of the contract or up to 90 days, whichever is less. The Installation Pass will be valid for the length of the contract, up to 2 years, or until the expiration date of the supporting document (for example, passport) that was used to obtain the Installation Pass, whichever is earliest.

d. Sponsor Requirements.

(1) Unlike people in other categories, identifying the sponsoring organization may be more difficult for this type of contractor. In general, the organization hiring the contractor will perform the sponsor responsibilities in this regulation. Hiring organizations will not request access for contractors that extends beyond their needs. For example, if an organization is going to have furniture delivered to two installations in a BSB, the hiring organization will not sponsor the contractor for an installation pass that allows access to more than the BSB.

(2) Sponsoring-organization requirements for various levels of access are as follows:

(a) When access to more than three ASGs is requested, the request will be considered the same as “USAREUR-wide.” Specifically, requests that include access to more than three ASGs may be approved only by the following organizations, which will perform sponsoring-organization responsibilities:

1. Department of Defense Dependents Schools-Europe.
2. Defense Commissary Agency, European Region.
3. Defense Logistics Agency, Europe.
4. Army and Air Force Exchange Service, Europe (AAFES-Eur).
5. Military Surface Deployment and Distribution Command, Europe.
6. United States Army Center for Health Promotion and Preventive Medicine - Europe.
7. United States Army Medical Materiel Center, Europe.
8. United States Army Corps of Engineers, Europe District.
9. IMA-E.
10. HQ USAREUR/7A staff offices.
11. V Corps.
12. 21st Theater Support Command.

13. United States Army Southern European Task Force.
14. Seventh Army Training Command.
15. 7th Army Reserve Command.
16. 266th Finance Command.
17. 1st Personnel Command.
18. 18th Engineer Brigade.
19. 5th Signal Command.
20. 66th Military Intelligence Group.
21. 202d Military Police Group.
22. United States Army Europe Regional Medical Command.
23. United States Army Europe Regional Dental Command.
24. United States Army Contracting Command, Europe.
25. United States Army Materiel Command, Europe.
26. 1st Theater Movement Control Agency.

NOTE: The USAREUR PM will adjudicate cases when an organization other than those listed above believes that it should have USAREUR-wide sponsoring authority.

(b) When access is required to two or three ASGs, the grade requirements of paragraph 30b(2)(c)4 apply; however, the sponsoring organization need not be one of the organizations in (a) above. The sponsoring organization will be the ASG where the contractor is headquartered or performs most of his or her business.

(c) Contractors whose service exceeds one BSB but is limited to one ASG may obtain an Installation Pass for that ASG. The sponsoring organization must be the ASG.

(d) In all other cases, sponsoring organizations are not authorized to sponsor an Installation-Pass applicant beyond the BSB.

(3) Contractors who are unable to obtain an Installation Pass based on the requirements in (2) above but who require access to installations throughout the USAREUR AOR based on individual contracts with several organizations should obtain an installation pass for the ASG or BSB where they conduct most of their business and use sign-in procedures or site-specific access rosters for other locations. Paragraph 42 explains access-roster requirements.

e. Background Checks.

(1) **PGCC (*Polizeiliches Führungszeugnis*)**. This certificate is required before a Temporary Installation Pass or Installation Pass may be issued.

(2) **MP Check**. This check is required before a Temporary Installation Pass or Installation Pass may be issued. (**NOTE:** This applies only to U.S. citizens.)

(3) **DCII**. If the applicant claims previous affiliation with the U.S. Armed Forces and has a social security number, this check must be completed before a Temporary Installation Pass or Installation Pass may be issued.

(4) FNS. This screening applies to both non-U.S. citizens and U.S. citizens who have lived in Germany for more than 12 consecutive months. This screening must be initiated before a Temporary Installation Pass is issued; it must be completed and returned negative, with no entries, before an Installation Pass is issued.

f. Residence and Work Permits. These permits may be required for non-German citizens, unless the non-German citizen has an exception to this requirement (para 30b(6)(d)).

g. Restrictions on Number of Installations a Pass Holder May Enter. The number of installations will be limited to the minimum required for the contractor to perform his or her duties, according to subparagraph d above.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions unless specified by the sponsor organization.

i. Restrictions on Sign-In Privileges. Sign-in privileges normally are not granted to contractors. As an exception, contractors may be granted sign-in privileges when the sponsoring official is at least a lieutenant colonel or civilian equivalent (GS-13 or C-8). The 22d ASG and 80th ASG may use the equivalent grade for their LN employees. Sign-in privileges are not authorized at FPCON Delta. Sign-in privileges, when authorized, will be limited to signing in four people and their vehicles. Only other contractors and vendors that support the contract may be signed in. Sign-in privileges are not authorized for Temporary Installation Pass holders.

j. FPCON Restrictions. The Temporary Installation Pass allows access during FPCON Alpha and FPCON Bravo. A one FPCON level increase may be granted by the IACO if requested by the sponsoring organization. There are no restrictions for the Installation Pass.

16. PERSONAL-SERVICE EMPLOYEE

a. Definition. An individual hired by someone (see “requester” in glossary) to perform a service (for example, as nanny, dog-sitter, house-cleaner).

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass may be authorized after all required background checks except the FNS have been completed (see e(4) below).

(2) Installation Pass. This pass may be authorized after all background checks (including an FNS) have been completed and returned negative, with no entries.

NOTE: Background checks that uncover entries must be forwarded to the host ASG for adjudication. ASG, BSB, and other commanders and security personnel will strictly control security checks and treat them as confidential. Responsible commanders will ensure that only persons with a need to know have access to individual security files (AR 381-45). Background checks with entries will be passed through security channels to the local U.S. commander of the employee for action. Paragraph 30b(5)(b) has additional guidance.

c. Length of Time Pass Is Valid. The Temporary Installation Pass is valid for the length of service or up to 90 days, whichever is earlier. The Installation Pass is valid for the length of service, for 2 years, or until the expiration date of the supporting document (for example, passport) that was used to obtain the installation pass, whichever is earliest.

d. Sponsor Requirements. The BSB where the requester resides will be the sponsor for this person and will perform the sponsor responsibilities.

e. Background Checks.

(1) PGCC (*Polizeiliches Führungszeugnis*). This certificate is required before a Temporary Installation Pass or Installation Pass may be issued.

(2) MP Check. This check is required before a Temporary Installation Pass or Installation Pass may be issued. (**NOTE:** This applies only to U.S. citizens.)

(3) **DCII.** If the applicant claims previous affiliation with the U.S. Armed Forces and has a social security number, this check is required before a Temporary Installation Pass or Installation Pass may be issued.

(4) **FNS.** This screening is required for non-U.S. citizens and U.S. citizens who have lived in Germany for more than 12 consecutive months. This screening must be initiated before a Temporary Installation Pass may be issued; it must be completed and returned negative, with no entries, before an Installation Pass is issued.

f. Residence and Work Permits. These permits may be required for non-German citizens, unless the non-German citizen has an exception to this requirement (para 30b(6)(d)).

g. Restrictions on Number of Installations a Pass Holder May Enter. Access may not exceed the sponsoring BSB. The sponsoring BSB may further restrict access as necessary. Access may be extended to the ASG if the ASG is willing to accept sponsoring-organization responsibilities.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on days and times access is authorized unless specified by the requester or sponsor.

i. Restrictions on Sign-In Privileges. Persons in this category are not authorized sign-in privileges.

j. FPCON Restrictions. The Temporary Installation Pass allows access during FPCON Alpha and FPCON Bravo. A one FPCON level increase may be granted by the IACO if requested by the sponsoring organization. There are no restrictions for the Installation Pass.

17. DELIVERY PERSONNEL (RECURRING DELIVERIES OR SIMILAR SERVICE NOT ASSOCIATED WITH A GOVERNMENT CONTRACT)

a. Definition. An individual who needs recurring access to U.S. Forces installations to make deliveries or perform a similar service that is related to his or her employment (for example, pizza delivery, taxi driver).

b. Type of Pass Authorized.

(1) **Temporary Installation Pass.** This pass is not authorized.

(2) **Installation Pass.** This pass may be authorized after all background checks (including an FNS) have been completed and returned negative, with no entries.

NOTE: Background checks that uncover entries must be forwarded to the host ASG for adjudication. ASG, BSB, and other commanders and security personnel will strictly control security checks and treat them as confidential. Responsible commanders will ensure that only persons with a need to know have access to individual security files (AR 381-45). Background checks with entries will be passed through security channels to the local U.S. commander of the employee for action. Paragraph 30b(5)(b) has additional guidance.

c. Length of Time Pass Is Valid. The Installation Pass will be valid for up to 2 years or expire on the expiration date of the supporting document (for example, passport) that was used to obtain the Installation Pass, whichever is earlier.

d. Sponsor Requirements. The BSB being serviced will be the sponsor for people in this category.

e. Background Checks.

(1) **PGCC (*Polizeiliches Führungszeugnis*).** This certificate is required before an Installation Pass may be issued.

(2) **MP Check.** This check must be completed before an Installation Pass may be issued. (**NOTE:** This applies only to U.S. citizens.)

(3) **DCII.** If the applicant claims a previous affiliation with the U.S. Armed Forces and has a social security number, this check is required before an Installation Pass may be issued.

(4) **FNS.** This screening is required for non-U.S. citizens and U.S. citizens who have lived in Germany for more than 12 consecutive months. It must be completed and returned negative, with no entries, before an Installation Pass is issued.

f. Residence and Work Permits. These permits are required for non-German citizens. Paragraph 30b(6)(d) explains exceptions to this requirement.

g. Restrictions on Number of Installations a Pass Holder May Enter. Installation Pass holders will not be granted access outside of the sponsoring BSB. The sponsoring BSB may impose further restrictions (for example, to only certain caserns). Access may be extended to the ASG only if the ASG is willing to accept sponsoring-organization responsibilities.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on when access is authorized unless specified by the sponsor.

i. Restrictions on Sign-In Privileges. Persons in this category are not authorized sign-in privileges.

j. FPCON Restrictions. Installation Passes for delivery personnel are valid only at FPCON Alpha and FPCON Bravo. A one FPCON level increase may be granted by the IACO if requested by the sponsoring organization.

18. VENDOR

a. Definition. An individual who is authorized to sell merchandise or provide services on U.S. Forces installations.

b. Type of Pass Authorized.

(1) **Temporary Installation Pass.** This pass is not authorized.

(2) **Installation Pass.** This pass may be authorized after all background checks (including an FNS) have been completed and returned negative, with no entries.

NOTE: Background checks that uncover entries must be forwarded to the host ASG for adjudication. ASG, BSB, and other commanders and security personnel will strictly control security checks and treat them as confidential. Responsible commanders will ensure that only persons with a need to know have access to individual security files (AR 381-45). Background checks with entries will be passed through security channels to the local U.S. commander of the employee for action. Paragraph 30b(5)(b) has additional guidance.

c. Length of Time Pass is Valid. The Installation Pass will be valid for up to 2 years, until the expiration date of the supporting document (for example, passport) that was used to obtain the Installation Pass, or until the expiration date of the vendor permit, whichever is earliest.

d. Sponsor Requirements. The sponsoring organization will be the BSB when access requested does not exceed the BSB. The sponsoring organization will be the ASG when access requested exceeds one BSB but is limited to one ASG. When access is for more than one ASG, the applicant must be sponsored by AAFES-Eur; Defense Commissary Agency, European Region; or IMA-E. This sponsoring authority may not be delegated to subordinate organizations.

e. Background Checks.

(1) **PGCC (*Polizeiliches Führungszeugnis*).** This certificate is required before an Installation Pass may be issued.

(2) **MP Check.** This check is required before an Installation Pass may be issued. (**NOTE:** This applies only to U.S. citizens.)

(3) **DCII.** If the applicant claims a previous affiliation with the U.S. Armed Forces and has a social security number, this check is required before an Installation Pass may be issued.

(4) **FNS.** This screening is required for both non-U.S. citizens and U.S. citizens who have lived in Germany for more than 12 consecutive months. This screening must be completed and returned negative, with no entries, before an Installation Pass may be issued.

f. Residence and Work Permits. These permits are required for non-German citizens, unless the non-German citizen is an exception to this requirement according to paragraph 30b(6)(d).

g. Restrictions on Number of Installations a Pass Holder May Enter. The number of installations a pass holder may enter will depend on the level of the sponsoring organization (d above).

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on access days or times unless specified by the sponsor.

i. Restrictions on Sign-In Privileges. Persons in this category are not authorized sign-in privileges.

j. FPCON Restrictions. Installation passes are only valid during FPCON Alpha and FPCON Bravo. A one FPCON level increase may be granted by the IACO if requested by the sponsoring organization.

19. NATO MEMBER

a. Definition. NATO military personnel, civilian employees, and their family members who reside in Germany or who meet the requirements in USAREUR Regulation 600-700. This category is designed for members of NATO Sending States (active-duty Belgian, British, Canadian, Dutch, and French military stationed in Germany) and should not be confused with the Host-Nation Military Member category in paragraph 20.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass is not authorized.

(2) Installation Pass. This pass is authorized for people in this category.

c. Length of Time Pass Is Valid. This pass will be valid for up to 5 years, for the length of the member's tour, or until the expiration date of the supporting document (for example, a military ID card) that was used to obtain the installation pass, whichever is earliest.

d. Sponsor Requirements.

(1) NATO Members Assigned to an International Military Headquarters, Activity, or Special Mission in Germany. The parent organization will sponsor people in this category.

(2) Active-Duty Belgian, British, Canadian, Dutch, and French Military Stationed in Germany (also known as Sending States). The security office from the Sending State will sponsor people in this category. The Sending State will submit a memorandum designating sponsoring officials to the USAREUR PM by e-mail (iacs@manupo.pmo.army.mil). The PM will post this memorandum to the restricted portion of the IACS Web site, where it will be available to all USAREUR IACOs. Individuals in this category may obtain an Installation Pass at any IACO. Because these individuals are stationed throughout Germany, the first visit to a U.S. Forces-controlled installation must be coordinated with the sponsoring organization and IACO to obtain an Installation Pass according to paragraph 30c.

(3) French and British Consular and Diplomatic Personnel Stationed in Germany. The U.S. Mission, Germany (U.S. Department of State), will sponsor people in this category. The U.S. Mission, Germany, will submit a memorandum designating sponsoring officials to the USAREUR PM. The PM will post this memorandum to the restricted portion of the IACS Web site, where it will be available to all USAREUR IACOs. Individuals in this category may obtain their Installation Pass at any IACO. The first visit of French and British consular and diplomatic personnel to a U.S. Forces-controlled installation must be coordinated with the sponsoring organization and the IACO to obtain an Installation Pass according to paragraph 30c.

e. Background Checks. Background checks are not required for people in this category.

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

g. Restrictions on Number of Installations a Pass Holder May Enter. There are no restrictions. NATO Members are automatically granted access to U.S. Forces installations and facilities. No justification for access will be required.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions when access is authorized.

i. Restrictions on Sign-In Privileges. People in this category will be limited to signing in four people and their vehicles.

j. FPCON Restrictions. No FPCON restrictions apply.

20. HOST-NATION MILITARY MEMBER

a. Definition. A member of the host-nation military who works or resides on a U.S. Forces-controlled installation in the nation they serve (for example, German soldiers in Germany, Italian soldiers in Italy). This category should not be confused with the NATO Member category (para 19), which is designed specifically for members of NATO Sending States (active-duty Belgian, British, Canadian, Dutch, and French military stationed in Germany).

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass is not authorized.

(2) Installation Pass. Persons in this category will receive an Installation Pass.

c. Length of Time Pass Is Valid. The Installation Pass for a Host-Nation Military Member will be valid for up to 5 years, for the length of the member's tour, or until the expiration date of the supporting document (for example, a military ID card) that was used to obtain the installation pass, whichever is earlier.

d. Sponsor Requirements. If the Host-Nation Military Member works for an organization that has a DOD representative, that organization will be the sponsoring organization and perform the sponsor responsibilities. If no such organization exists, the BSB will perform the sponsor responsibilities.

e. Background Checks. No background checks are required for people in this category.

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

g. Restrictions on the Number of Installations a Pass Holder May Enter. The number of installations a pass holder may enter will be limited to the minimum required based on the Host-Nation Military Member's circumstances.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on access times unless specified by the sponsor.

i. Restrictions on Sign-In Privileges. Installation-Pass holders are not authorized sign-in privileges unless sign-in privileges are justified by the sponsoring organization. If sign-in privileges are justified by the sponsoring organization, the Installation-Pass holder may sign in up to four individuals and their vehicles "for official business only." Sign-in privileges for Installation-Pass holders in this category are not authorized during FPCON Delta.

j. FPCON Restrictions. No FPCON restrictions apply.

21. FOREIGN STUDENT (MARSHALL CENTER)

a. Definition. Foreign military students assigned to the George C. Marshall European Center for Security Studies in Garmisch, Germany.

b. Types of Pass Authorized.

(1) Temporary Installation Pass. This pass is not authorized.

(2) Installation Pass. This pass is authorized for people in this category.

c. Length of Time Pass Is Valid. The Installation Pass will be valid for up to 2 years, for the length of the student's tour, or until the expiration date of the supporting document (for example, military ID card) that was used to obtain the Installation Pass, whichever is earliest.

d. Sponsor Requirements. Representatives from the Marshall Center will perform the sponsor responsibilities.

e. Background Checks. No background check is required for people in this category.

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

g. Restrictions on Number of Installation a Pass Holder May Enter. Access will not exceed installations in the Garmisch AST.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions of days or times of access.

i. Restrictions on Sign-In Privileges. People in this category are not authorized sign-in privileges.

j. FPCON Restrictions. No FPCON restrictions apply.

22. MEMBER OF PRIVATE ORGANIZATION

a. Definition. A member of an approved private organization who has no other reason to enter U.S. Forces installations other than to participate in private-organization functions.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass is not authorized.

(2) Installation Pass. This pass may be authorized after all background checks (including an FNS) have been completed and returned negative, with no entries.

NOTE: Background checks that uncover entries must be forwarded to the host ASG for adjudication. ASG, BSB, and other commanders and security personnel will strictly control security checks and treat them as confidential. Responsible commanders will ensure that only persons with a need to know have access to individual security files (AR 381-45). Background checks with entries will be passed through security channels to the local U.S. commander of the employee for action. Paragraph 30b(5)(b) has additional guidance.

c. Length of Time Pass Is Valid. The Installation Pass will be valid for up to 2 years or until the expiration date of the supporting document (for example, passport) that was used to obtain the Installation Pass, whichever is earlier.

d. Sponsor Requirements. The BSB where the private-organization function takes place will perform sponsor responsibilities.

e. Background Checks.

(1) PGCC (*Polizeiliches Führungszeugnis*). This certificate is required before an Installation Pass may be issued.

(2) MP Check. This check must be completed before an Installation Pass is issued. (**NOTE:** This applies only to U.S. citizens.)

(3) DCII. If the applicant claims a previous affiliation with the U.S. Armed Forces and has a social security number, this check is required before an Installation Pass may be issued.

(4) FNS. This screening is required for non-U.S. citizens and U.S. citizens who have lived in Germany for more than 12 consecutive months. This screening must be completed and returned negative, with no entries, before an Installation Pass may be issued.

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

g. Restrictions on Number of Installations a Pass Holder May Enter. Access will not exceed the sponsoring BSB. The sponsoring BSB may impose further restrictions. Access may be extended to the ASG if the ASG is willing to accept sponsoring-organization responsibilities.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on days and times of access unless imposed by the sponsoring BSB.

i. Restrictions on Sign-In Privileges. People in this category are not authorized sign-in privileges.

j. FPCON Restrictions. Installation Passes are valid only during FPCON Alpha and FPCON Bravo. A one FPCON level increase may be granted by the IACO if requested by the sponsoring organization.

23. VISITOR (IMMEDIATE FAMILY MEMBER LIVING IN EUROPE)

a. Definition. An individual, age 10 and older, who is an immediate family member of the requester (glossary) and lives in Europe. In this regulation, “immediate family members” include the requester’s son, daughter, mother, father, brother, sister, mother-in-law, father-in-law, brother-in-law, sister-in-law, grandparents, and grandparents-in-law.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass is not authorized.

(2) Installation Pass. This pass may be authorized only when the requester resides on a controlled-access installation.

c. Length of Time Pass Is Valid. The Installation Pass will be valid until the expiration date of the requester’s ID-card or the expiration date of the supporting document (for example, passport) that was used to obtain the installation pass, whichever is earlier.

d. Sponsor Requirements. The BSB where the requester resides will be the sponsor for people in this category and will perform sponsor responsibilities.

e. Background Checks. No background checks are required for people in this category.

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

g. Restrictions on Number of Installations a Pass Holder May Enter. Access will not exceed the sponsoring BSB. The sponsoring BSB may impose further restrictions. A valid visitor installation-pass holder, when accompanied by the requester, will be authorized access when the individual must temporarily exceed his or her access level.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on when access is authorized unless specified by the requester or sponsor.

i. Restrictions on Sign-In Privileges. People in this category are not authorized sign-in privileges.

j. FPCON Restrictions. Installation passes will be valid only during FPCON Alpha and FPCON Bravo. A one FPCON level increase may be granted by the IACO if requested by the sponsoring organization.

24. VISITOR (FRIEND OR FAMILY MEMBER NOT INCLUDED IN CATEGORY ABOVE)

a. Definition. A visiting family member or friend, age 10 and older, of the requester (glossary) who is not included in the category in paragraph 23. Applicants must prove that they are staying with the requester and have an established departure date. This category will not be used to allow local friends or local people who are not immediate family members unescorted access to U.S. Forces installations.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. People in this category may be issued a Temporary Installation Pass.

(2) Installation Pass. People in this category may be issued an Installation Pass only if they are family members.

c. Length of Time Pass Is Valid. The Temporary Pass will be valid for the length of the visit or up to 90 days, whichever is less. An Installation Pass will be valid for the length of the visit (more than 90 days), up to 1 year, or until the expiration date of the supporting document (for example, passport) that was used to obtain the installation pass, whichever is earliest.

d. Sponsor Requirements. The BSB where the requester resides will be the sponsor for people in this category and will perform the sponsor responsibilities.

e. Background Checks. Background checks are not required for people in this category.

f. Residence and Work Permits. A residence permit will be required if an Installation Pass is going to be issued for more than 90 days.

g. Restrictions on Number of Installations a Pass Holder May Enter. Passes will not exceed the sponsoring BSB. The sponsoring BSB may impose further restrictions. Access may be extended to the ASG only if the ASG is willing to accept sponsoring-organization responsibilities. A valid visitor installation-pass holder, when accompanied by the requester, will be authorized access when the individual must temporarily exceed his or her access level.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on when access is authorized unless imposed by the requester or sponsor.

i. Restrictions on Sign-In Privileges. People in this category are not authorized sign-in privileges.

j. FPCON Restrictions. Installation passes will be valid only during FPCON Alpha and FPCON Bravo. A one FPCON level increase may be granted by the IACO if requested by the sponsoring organization.

25. OFFICIAL GUEST

a. Definition. A broad category designed for individuals requiring recurring access for official business, access based on an official relationship, a co-use agreement with the U.S. Government (for example, official visits from other Federal agencies), membership in clubs or organizations located on an installation (for example, shooting clubs, dance clubs, glider clubs), or individuals *in loco parentis*. Sponsoring organizations will not use this category when the applicant meets the definition of another, more restrictive category.

NOTE: Individuals requiring access due to *in loco parentis* status or other Member of Household statuses are required to submit a copy of the official memorandum from the Host Nation Customs Policy Branch, Office of the Provost Marshal, HQ USAREUR/7A; or the AE Form 600-700A.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. People in this category may be issued Temporary Installation Passes.

(2) Installation Pass. People in this category may be issued an Installation Pass.

c. Length of Time Pass Is Valid. A Temporary Installation Pass will be valid for up to 90 days. An Installation Pass will be valid for up to 2 years, until the expiration date of the supporting document (for example, passport) that was used to obtain the Installation Pass; or until the expiration date of the agreement, memorandum, or membership, whichever is earliest.

d. Sponsor Requirements. The sponsoring organization will depend on the type of official guest. In most cases, the ASG or BSB will be the sponsor for people in this category and will perform the sponsor responsibilities.

e. Background Checks. The sponsoring ASG or BSB will determine whether or not a background check is required.

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

g. Restrictions on Number of Installations a Pass Holder May Enter. The number of installations will be limited to the minimum required.

h. Restrictions on Days and Times Access Is Authorized. Access times and dates will be as specified by the sponsoring organization.

i. Restrictions on Sign-In Privileges. People in this category will not be authorized sign-in privileges unless justified by the sponsoring organization. If authorized, sign-in privileges will be limited to signing in four individuals and their vehicles “for official business only.”

j. FPCON Restrictions. Installation passes will be valid only through FPCON Charlie; however, a one FPCON level increase may be granted by the IACO if requested by the sponsoring organization.

26. DEPARTMENT OF STATE AND AMERICAN EMBASSY PERSONNEL

a. Definition. An individual assigned to or on duty with the United States Department of State, an American Embassy in the USEUCOM AOR, or in U.S. diplomatic or consular posts according to USAREUR Regulation 600-700.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass is not authorized.

(2) Installation Pass. People in this category may be issued an Installation Pass.

c. Length of Time Pass Is Valid. The Installation Pass will be valid for the length of the tour (not to exceed 5 years) or until the expiration date on the supporting document (for example, passport, AE Form 600-700A) that was used to obtain the Installation Pass, whichever is earlier.

d. Sponsor Requirements. The United States Mission, Germany, will be the sponsor for people in this category and will perform the sponsor responsibilities. The United States Mission, Germany, will submit a memorandum designating sponsoring official to the USAREUR PM by e-mail (iacs@manupo.pmo.army.mil). The PM will post this memorandum to the restricted portion of the IACS Web site, where it will be available to all USAREUR IACOs. Individuals in this category may obtain their Installation Pass at any IACO. Because these individuals are spread throughout Europe, their first visit to a U.S. Forces-controlled installation must be coordinated with the sponsoring organization and IACO to obtain the Installation Pass according to paragraph 30b.

e. Background Checks. Background checks are not required for people in this category.

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

g. Restrictions on Number of Installations a Pass Holder May Enter. There are no restrictions on the number of installations. Department of State and American Embassy personnel automatically receive access to U.S. Forces installations. No justification is required.

h. Restrictions on Days and Times Access Is Authorized. There are no restrictions on when people in this category may access installations.

i. Restrictions on Sign-In Privileges. People in this category will be limited to signing in four people and their vehicles.

j. FPCON Restrictions. No FPCON restrictions apply.

27. OTHER

a. Definition. An individual who requires recurring and unescorted access, but who does not meet the definition of another category in paragraphs 12 through 26, 28, or 29. Sponsoring organizations will not use this category if the applicant meets the definition of another, more restrictive category. An example for this category would be people who transport U.S. Forces employees to and from work on a daily basis.

b. Type of Pass Authorized.

(1) Temporary Installation Pass. People in this category may be issued a Temporary Installation Pass.

(2) Installation Pass. People in this category may be issued an Installation Pass.

c. Length of Time Pass Is Valid. A Temporary Installation Pass will be valid for up to 90 days. An Installation Pass will be valid for 1 year or until the expiration date on the supporting document (for example, passport) that was used to obtain the Installation Pass, whichever is earlier.

d. Sponsor Requirements. The BSB where access is required will be the sponsor for people in this category and will perform the sponsor responsibilities.

e. Background Checks. The sponsoring BSB will determine whether or not a background check is required.

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

g. Restrictions on Number of Installations a Pass Holder May Enter. Access will not exceed the sponsoring BSB. The sponsoring BSB may impose further restrictions. Access may be extended to the ASG only if the ASG is willing to accept sponsoring-organization responsibilities.

h. Restrictions on Days and Times Access Is Authorized. The sponsoring BSB will determine restrictions on when access may be granted.

i. Restrictions on Sign-In Privileges. People in this category will not be authorized sign-in privileges.

j. FPCON Restrictions. Installation passes will be valid only during FPCON Alpha and FPCON Bravo. A one FPCON level increase may be granted by the IACO if requested by the sponsoring organization.

28. HOST-NATION GOVERNMENT OFFICIAL

a. Definition. A member of the host-nation Government who requires recurring access for official business or access based on an official relationship, or visits by local city officials (such as the mayor, fire chief, or an employee of the German Construction Office (*Bauamt*)).

b. Type of Pass Authorized.

(1) Temporary Installation Pass. This pass is not authorized.

(2) Installation Pass. People in this category may be issued an Installation Pass.

c. Length of Time Pass Is Valid. An Installation Pass will be valid for up to 5 years or until the expiration date of the supporting document (for example, passport) that was used to obtain the Installation Pass, whichever is earlier.

d. Sponsor Requirements. The sponsoring organization will depend on the type of official guest. In most cases, the ASG or BSB will be the sponsor for people in this category and will perform the sponsor responsibilities.

e. Background Checks. Background checks are not required for people in this category.

NOTE: Persons and firms contracted by the host nation will be screened as Contractor (Living in Host Nation) and will have the background check requirements in paragraph 15e.

f. Residence and Work Permits. People in this category are not required to have residence or work permits.

g. Restrictions on Number of Installations a Pass Holder May Enter. The number of installations will be limited to the minimum required for the guest to conduct official business.

h. Restrictions on Days and Times Access Is Authorized. Access times and dates will be as specified by the sponsoring organization.

i. Restrictions on Sign-In Privileges. People in this category will not be authorized sign-in privileges unless justified by the sponsoring organization. If authorized, sign-in privileges will be limited to signing in four individuals and their vehicles “for official business only.”

j. FPCON Restrictions. Installation passes will be valid only through FPCON Charlie; however, a one FPCON level increase may be granted by the IACO if requested by the sponsoring organization.

29. GATE GUARD

a. Definition. A guard in the position of controlling access to the installation. Typically, these are contracted positions where guards do not require access to the installation themselves; they conduct their work only from the ACP. This category is reserved only for logical access (glossary). Gate guards authorized and requiring installation access for the purpose of their work will be issued installation passes under the Contractor (Living in Host Nation) person category.

b. Type of Pass Authorized.

(1) **Temporary Installation Pass.** This type of pass is not authorized.

(2) **Installation Pass.** People in this category may be issued an Installation Pass.

c. Length of Time Pass Is Valid. An Installation Pass will be valid for up to 2 years or until the expiration date of the supporting document (for example, passport) that was used to obtain the Installation Pass, whichever is earlier.

d. Sponsor Requirements. The sponsoring organization will be the contracting officer's representative (COR) or the ASG site contracting officer's representative (SCOR).

e. Background Checks. Background checks are assumed to have been completed, verified, and adjudicated per AR 190-56 and AE Regulation 190-13, chapter 7, by the COR or SCOR as a condition of employment. Additional background checks are not required for people in this category.

f. Residence and Work Permits. Appropriate residence or work permits are assumed to have been verified by the COR or SCOR as a condition of employment.

g. Restrictions on Number of Installations a Pass Holder May Enter. Only logical access is granted.

h. Restrictions on Days and Times Access Is Authorized. Only logical access is granted.

i. Restrictions on Sign-In Privileges. Sign-in privileges are not authorized.

j. FPCON Restrictions. No restrictions.

**SECTION IV
INSTALLATION PASS**

30. APPLICATION PROCESS

a. Sponsoring officials will help authorized individuals apply for an installation pass at the servicing IACO by preparing AE Form 190-16A (app C). AE Form 190-16A must be completed for the following reasons:

- (1) To receive an initial installation pass (first-time pass).
- (2) To renew a pass that has expired or is about to expire (para 32).
- (3) To replace a pass that was lost or stolen (para 33).
- (4) To extend a Temporary Installation Pass (para 34).
- (5) To replace an unserviceable pass (para 35).

NOTE: Applications must be completed in English using standard American measurements. Appendix D is a height and weight conversion chart.

b. Key components of the application process include the following:

(1) **Sponsoring Organization.** The sponsoring organization will designate individuals in its organization to take care of the sponsoring organization's responsibilities. The sponsoring organization for each applicant is based on the applicant's category (paras 12 through 29). For example, the BSB will serve as the sponsoring organization for some applicants; the hiring organization will serve as the sponsoring organization for other applicants.

(2) **Sponsoring Official.**

- (a) The sponsoring official is key to the integrity of the Installation Access Control Program.

(b) The commander or first lieutenant colonel or civilian equivalent (GS-13) in the chain of command of an organization that sponsors installation-pass applicants will designate sponsoring officials in writing. If the sponsoring organization does not have this military or civilian pay-grade structure (for example, military banking facilities, Government travel agency), the local senior manager or deputy of the organization is authorized to sign the designation memorandum. Sponsoring organizations without a military or civilian pay-grade structure must ensure that the application does not authorize access beyond the BSB. Sponsoring organizations will ensure the organization's security manager delivers the sponsoring official designation memorandum (app B) to the servicing IACO. The IACO will—

1. File and maintain the memorandum.

2. Use the memorandum to verify the authorization of the sponsoring official each time an individual applies for an installation pass and to verify that the appropriate organization is listed as the sponsoring organization.

(c) Sponsoring officials must be DOD ID-card holders or full-time LN employees. The following are minimum grade requirements and limits on the sponsoring official's approving authority:

1. Supervisor who is a sergeant first class or chief warrant officer 2, or civilian employee in pay grade of GS-9 or C-6A: authorized to sponsor individuals for only single-installation access.

2. Supervisor who is a first sergeant or master sergeant, chief warrant officer 3, captain, or civilian employee in pay grade of GS-11, NF 4, or C-7: authorized to sponsor individuals for BSB access.

3. Supervisor who is a sergeant major, major, chief warrant officer 4, or civilian employee in pay grade GS-12, NF 4, or C-7A: authorized to sponsor individuals for ASG access.

4. Supervisor who is a lieutenant colonel or civilian employee in pay grade GS-13, NF 5, or C-8: authorized to sponsor individuals for U.S. Forces-wide access. Paragraph 15d provides additional restrictions for applicants in the Contractor (Living in Host Nation) category.

NOTE: The 22d ASG and 80th ASG may use equivalent pay-grade structures for their LN employees.

(d) NATO Sending States and the United States Mission, Germany, will submit their sponsoring-official-designation memorandum to the USAREUR PM. The PM will post this memorandum to the restricted portion of the IACS Web site, where it will be available to all USAREUR IACOs. IACOs will honor any memorandum posted to the IACS Web site, regardless of the requirements in (b) and (c) above.

(e) Sponsoring officials will ensure the requirements and intent of this regulation are followed.

(3) Category. An applicant's category will determine the type of installation pass that may be issued and the associated restrictions. Sponsoring officials will state the category on the application (block 7); IACO registrars will verify its correctness. The registration requirements and restrictions vary among categories.

(4) Type of Installation Pass Requested. Sponsors will request either the Temporary Installation Pass or Installation Pass based on the applicant's category and the circumstances under which the applicant is applying.

(5) Background Checks.

(a) Background checks are used to determine if an applicant is a security risk. Background-check requirements are based on an individual's category. Sponsoring organizations are responsible for completing required background checks. IACO registrars will require verification that a background check has been completed or, when applicable, that a background check has been initiated. Sponsoring organizations should refer to the appropriate category (paras 12 through 29) to determine the exact background-check requirements for each applicant.

(b) Background checks that uncover no derogatory information will be forwarded to the sponsoring organization. Background checks that uncover derogatory information will be forwarded to the sponsoring organization and to the host ASG. The ASG will coordinate with the sponsoring organization to determine whether the derogatory information warrants denial of access privileges. If the requested access is for more than one ASG, the USAREUR PM must be consulted. When determining whether or not derogatory information should warrant denial of access privileges, ASGs and sponsoring organizations will consider both the seriousness of the derogatory information and when the incident or offense occurred.

(c) The following explains the types of background checks used for installation passes:

1. PGCC (*Polizeiliches Führungszeugnis*). The applicant will get this certificate from his or her city ordinance office (*Ordnungsamt*). The certificate is based on records available to the German Government and should have “No Record of Misconduct (*Keine Eintragung*)” stamped on the bottom. A translation must be obtained for any other annotations. Certificates that are more than 12 months old may not be used. If not qualified for the German *Polizeiliches Führungszeugnis* (based on less than 1 year of residency in Germany), a PGCC equivalent will be required from the previous country of residence and it must be translated into English.

NOTE: Some non-German contractors with Technical Expert status who must obtain an installation pass may not be able to obtain the PGCC (*Polizeiliches Führungszeugnis*) because they have not established their regular residency in Germany. In these cases, contact USAREUR PM for guidance.

2. MP Check. Sponsoring officials will obtain an MP-records check from their servicing MP station. (**NOTE:** This applies only to U.S. citizens.)

3. DCII. The DCII is the automated central repository that identifies investigations conducted by DOD investigative agencies and shows personnel security determinations made by DOD adjudicative authorities. The DCII database consists of an index of personal names and impersonal titles that appear as subjects, co-subjects, victims, or cross-referenced incidental subjects in investigative documents maintained by DOD criminal, counterintelligence, fraud, and personnel-security investigative activities. DOD investigative and adjudicative authorities report information that is used for investigative, adjudicative, statistical, research, and other purposes as authorized. The DCII is only for individuals with social security numbers who have had affiliation with the U.S. Forces. Sponsoring officials may coordinate with their organization’s security manager to determine the nearest DCII-access terminal. If an individual has a current security clearance, a check of the DCII is unnecessary.

4. FNS. The USAREUR PM uses the Foreign National Screening Program to ensure only suitable foreign nationals are granted access to installations. An FNS may also be conducted on U.S. citizens who have lived in Germany for an extended period. The USAREUR G2 manages this program. Sponsoring organizations will comply with FNS procedures in USAREUR Regulation 604-1. Documentation showing that the FNS has been initiated (required in some cases before issuing a Temporary Installation Pass) or that it has been completed may be obtained from the FNS Web site (<https://144.170.184.21/newweb/fnsp/>). Questions about FNS should be addressed to the unit or organization security officer.

NOTE: The AE Form 604-1B (available at <https://www.aeaim.hqusareur.army.mil/library/for/index-aeef.shtm>) must be signed by the individual that the FNS is being conducted on. It does not, however, need to be turned into the IACO as part of the application packet.

(d) It is not uncommon for an applicant to be ineligible to have a required background check completed because of the applicant’s country of residence or length of time the applicant has lived in Germany. For instance, an applicant must have lived in Germany during the past 12 or more months for an FNS to be initiated. Applicants in the Vendor category who come from other countries to sell their merchandise often have this problem. Although a BSB has the authority to deny an installation pass based on its inability to conduct background checks and properly clear the applicant, BSBs should handle each situation individually and make a determination based on a risk assessment. BSBs can reduce their risks by using one or more of the following strategies:

1. If the applicant is not a German resident, require the applicant to provide his or her country’s equivalent of the PGCC and require this document to be in English and notarized.

2. More closely scrutinize access requirements and limit the number of installations and times when access is allowed.

3. If the person category allows sign-in privileges, deny these privileges to anyone who cannot provide adequate background-check information.

4. Limit the duration of the installation pass to coincide with the date when the individual will have 12 months of residency in Germany and a FNS can be conducted.

(6) Residence and Work Permits.

(a) As a rule, any non-German citizen may work for the U.S. Armed Forces in Germany if he or she has a residence permit (*Aufenthaltsberechtigung*, *Aufenthaltserlaubnis*, or *Aufenthaltsbewilligung*) and a work permit (*Arbeitslaubnis*).

(b) Installation-Pass applicants must have residence and work permits before receiving an Installation Pass unless the applicant is exempt from this requirement according to (d) below.

(c) If indicated in the registration requirements of the person's category, non-German citizens and contractors in Germany who work for DOD must submit a copy of their residence and their work permits. The residence permit is stamped in the passport. The work permit is issued on a separate form.

NOTE: A residence permit is required if staying longer than 90 consecutive days.

(d) Citizens of EU-member states are exempt from the work-permit requirement. They should, however, have an EU residence permit (separate form) if they have established their permanent residence in Germany. The following types of individuals are also exempt from the work-permit requirement:

1. Soldiers, members of the civilian component, and employees of organizations or contractors who have status under Articles 71 through 73, NATO Status of Forces Agreement (SOFA) Supplementary Agreement.

2. Non-German citizens who are family members of U.S. Armed Forces personnel or family members of personnel who are assigned to the civilian component.

3. Students at German universities coming from non-EU countries if they work less than 3 months during the university's vacation period. They must, however, have a residence permit.

(7) Number of Installations to Which Access Is Required.

(a) One of the main objectives of the Installation Access Control Program is to limit access to the minimum number of installations based on individual requirements.

(b) The following categories will be granted U.S. Forces-wide access in the USAREUR AOR without being required to provide justification:

1. DOD ID-Card Holder (para 12).

2. NATO Member (para 19).

3. Department of State and American Embassy Personnel (para 26).

(c) If justification is required for an individual to gain access to installations in the USAREUR AOR, the individual's sponsoring official will—

1. Ensure the application lists the minimum number of installations to which access is required by listing the specific name of the ASG, BSB, or installations (for example, only Taylor Barracks and Coleman Barracks, only 293d BSB). If access is required to more than one BSB or installation, provide detailed justification.

2. If an applicant in Germany requires "USAREUR-wide" access, indicate whether the requirement is only for Army installations or will include U.S. Air Force installations. Also, the application must specify whether access is required at the 22d ASG and 80th ASG. If access is required in the 22d ASG AOR, the application must include written permission from the 22d ASG PMO.

(d) If justification is required for an individual to enter installations in the USAREUR AOR, the IACO issuing official will—

1. Ensure the level of access requested does not exceed the sponsoring official's authority.

2. Clarify inadequate justifications by coordinating with the sponsoring official.

3. Carefully examine all applications for individuals under the Contractor (Living in Host Nation) category to ensure the requested level of access meets requirements in paragraph 15.

(8) Days and Times Access Is Required. Sponsoring officials will ensure the application shows the minimum days and times access is required.

(9) Sign-in Privileges. Sponsoring officials may request sign-in privileges for the applicant only if bona fide justification is available. This justification must extend beyond convenience for the installation-pass holder or sponsoring organization and it must clearly explain why the installation-pass holder requires sign-in privileges. In most cases, sign-in privileges will be limited to other contractors and individuals on official business, not for personal business. The only exceptions are people in the NATO Member category (para 19) and Department of State and American Embassy Personnel (para 26) category, who receive automatic sign-in privileges.

(a) Installation-Pass holders with sign-in privileges will follow the sign-in procedures in paragraph 41.

(b) IACO registrars will ensure the military and civilian grade requirements of the sponsoring official are met when sign-in privileges are requested for contractors in the Contractor (Living in Host Nation) category (para 15d).

(c) Sign-in privileges will never be authorized for Temporary Installation Pass holders.

(d) People in categories with authorized sign-in privileges may sign in no more than four individuals and their vehicles.

(10) FPCON Restrictions. FPCON restrictions are based on an individual's category. The IACS will prohibit access beyond the FPCON associated with the category (paras 12 through 29). If sponsoring officials want to further restrict access at any of the FPCON levels, the application must specify the restriction.

(11) Vehicle Information. All individuals applying for an Installation Pass will register the vehicles they use to enter U.S. Forces installations in the USAREUR AOR. Only POVs are required to be registered and associated with an applicant's IACS record, not company vehicles. Proof of ownership is not required for the purpose of registering in IACS and will never be grounds to deny issuance of a regular or temporary pass. The following vehicle information must be included in blocks 24 and 25 of the application (AE Form 190-16A):

(a) License-plate number and country of issue.

(b) Make, model, year, body type, and color.

(c) Company's name and telephone number (only for Contractor (Living in Host Nation) category).

c. When the application is complete, the sponsoring official will escort the applicant to the servicing IACO with the required documentation (d below). If the sponsoring official cannot escort the applicant and the applicant has no other means of obtaining access to the installation, the following procedures are authorized:

(1) The sponsoring official will send the application by e-mail to the servicing IACO and inform the issuing official of the approximate date and time the applicant will come to the installation.

(2) The IACO issuing official will verify that the e-mail is from an authorized sponsoring official by checking the memorandum designating sponsoring officials from the sponsoring organization.

(3) When the applicant arrives at the ACP, the guard will call the IACO to verify that the applicant is expected and that the IACO has received an e-mail from the sponsoring organization.

(4) The guard will check the applicant's passport or personal ID card (whichever is listed in the signed application that the applicant must have in his or her possession) and grant the applicant unescorted access.

(5) The applicant will take the signed original copy of the application to the servicing IACO and obtain an installation pass.

NOTE: Applicants will use similar procedures if they obtain access to the installation, but the sponsoring official is unable to escort them to the IACO. Under no circumstances will the applicant obtain an installation pass from the IACO without either the sponsoring official's presence or previous coordination with the IACO.

d. Applicants will submit the following documentation with the application:

(1) A copy of one of the following:

(a) Passport.

(b) Personal ID card issued by the country of citizenship (for example, German *Personalausweis*, Belgian Identity Card, Italian *carta d'identita*).

(c) Military ID card issued by one of the NATO Sending States (Belgium, Canada, France, the Netherlands, United Kingdom).

(2) A copy of all required background-check results.

(3) Verification that the applicant has a residence permit and a work permit, if required.

(4) A copy of the agreement (club membership, *in loco parentis* memorandum, AE Form 600-700A, contract) justifying the need for installation access and verification of expiration date.

NOTE: The applicant is not required to provide a photograph.

31. APPLICATION PROCEDURES FOR APPLICANT WITH TEMPORARY INSTALLATION PASS

a. These procedures do not require the sponsoring organization to submit a new application.

b. Sponsoring officials will notify the IACO either in person or by e-mail where the Temporary Installation Pass was issued and when the FNS was completed.

c. If the notification is by e-mail, the IACO issuing official will verify that the e-mail is from an authorized sponsoring official by checking the memorandum designating sponsoring officials from the sponsoring organization (app B).

d. The IACO notification must include the date the FNS was completed and that the results include no derogatory information. If derogatory information is found, the notification must state that the host ASG and sponsoring official have reviewed the results and determined that there is no derogatory information present to warrant denial of installation-access privileges. The notification will also include any other changes the sponsoring official wants to make since the Temporary Installation Pass was issued.

e. When the notification is received, the applicant will return the Temporary Installation Pass and obtain an Installation Pass. The notification paperwork will be filed with the original Temporary Installation Pass application packet.

32. APPLICATION PROCEDURES FOR RENEWAL PASS

a. Renewal requests must be submitted on a new application (AE Form 190-16A) from the sponsoring organization to validate the information on the original application.

b. The following applies to background checks when an applicant renews an Installation Pass:

(1) A new PGCC will be required if both of the following apply:

(a) A certificate was required based on the person's category. This requirement does not apply to people in the Local National Employee category (para 13).

(b) The previous certificate is more than 12 months old.

(2) A new MP check will be required if one was initially required based on the person's category. (People in the Local National Employee category (para 13) hired before 3 October 1985 were exempt, therefore they will not need a new MP check.)

(3) A new DCII will be required if one was initially required based on the person's category.

(4) Unless extraordinary circumstances exist, a new FNS will not be required. Sponsoring officials will use the verification from the original FNS.

c. Applicants will turn in the expiring or expired Installation Pass or an AE Form 190-16B receipt for it (if access control personnel confiscated an expired pass) before receiving a new Installation Pass.

NOTE: People in the Local National Employee category (para 13) who are transferring from one organization of the U.S. Forces to another without a break in service retain their status and will not be required to provide either a new PGCC or a new MP check. These transfers will be identified on the new application.

33. APPLICATION PROCEDURES FOR LOST OR STOLEN PASS

If an installation pass is lost or stolen, the installation-pass holder must immediately report it to the local MP station and IACO. The installation pass will be flagged in the IACS as lost or stolen. The sponsoring organization must submit a new application to the same IACO where the original installation pass was obtained. If requested by the sponsoring official in the application, the expiration date of the installation pass may be extended to show a full registration period for that individual's category.

34. APPLICATION PROCEDURES FOR EXTENSION OF TEMPORARY PASS

a. A Temporary Installation Pass may be extended only once for no more than 90 days with reasonable justification. The primary intent of allowing an extension is to provide Temporary Installation Pass holders with continued access when there is an unforeseen delay in receiving FNS results. If the FNS returns with derogatory information that warrants denial of an Installation Pass, the Temporary Installation Pass holder will not be issued another Temporary Installation Pass. Background checks with derogatory information will be processed according to paragraphs 5c(4), 5e(4), 5h(2), 5i(1), and 5k(3).

b. The sponsoring official will coordinate with the IACO that issued the Temporary Installation Pass. After the extension is approved by the issuing official, the Temporary Installation Pass holder will return to the IACO, return the original Temporary Installation Pass, and obtain a new Temporary Installation Pass with a new expiration date.

c. If the reason for the extension request is a delay in the FNS results, the issuing official will coordinate with the appropriate S-2 or security manager to determine the FNS status.

d. The one-time extension in subparagraph a above will not be used to circumvent the more stringent requirements of an Installation Pass.

e. Only the USAREUR PM may grant permission to re-extend a Temporary Installation Pass after the first 90-day extension (180 days), even if FNS results have not been received.

35. UNSERVICEABLE PASS

An unserviceable installation pass may be exchanged, one-for-one, at the pass holder's servicing IACO without action from the sponsoring organization. The pass holder will return the unserviceable installation pass unless the pass was confiscated by an MP official or access-control personnel (para 44a(4)). If the pass was confiscated by an MP official or access-control personnel, the receipt (AE Form 190-16B) will be used to obtain a new pass (fig 2). The expiration date on the replacement pass will be the same as that on the original installation pass.

SECTION V INSTALLATION ACCESS CONTROL OFFICE

36. GENERAL

a. Only USAREUR-approved IACOs are authorized to issue installation passes. A complete list of authorized IACOs is available at <http://www.hqusareur.army.mil/opm/iacs/Resources/USAREURIACSRegistrationStations.pdf>.

RECEIPT FOR CONFISCATED ID CARD (AE Reg 190-16)	
Mr./Mrs./Miss <u>Joe M. Smith</u>	
This is a receipt for your ID card. The ID card must be turned in. It is invalid because it—	
<input checked="" type="checkbox"/> is mutilated	<input type="checkbox"/> is expired
<input type="checkbox"/> has been obviously altered	
It has no further use. It is Government property. Access-control personnel are authorized by AR 600-8-14 to confiscate invalid Government cards. Please contact the proper installation authority for card replacement. This ID card will be turned over to the local military law enforcement activity for disposition.	
Card number 123-45-6789	Date confiscated 1 January 2005
Signature (access-control personnel)	
Location and name of facility 293d BSB, Mannheim, Sullivan Barracks ACP	
AE FORM 190-16B, MAR 05 Previous editions are obsolete.	

Figure 2. Sample AE Form 190-16B

b. With the exception of certain default settings in the IACS, IACOs have few limits on the type of installation passes that may be issued. For example, every IACO is authorized to issue a USAREUR-wide installation pass. This authority is based on the assumption that each IACO will follow the policy, procedures, and intent of this regulation and that the USAREUR PM will monitor the IACS activity.

c. Access control is an installation commander's responsibility. Organizations outside the direct control of the ASG and BSB will neither be authorized to issue installation passes nor will they be equipped with the IACS.

d. Authorized IACOs will be approved before the IACS is operational. Requests for additional IACOs or IACS-registration stations must be submitted through command channels to the USAREUR PM (AEAPM-O-SO), Unit 29931, APO AE 09086-9931.

e. BSBs should functionally align their IACO under their servicing PMO.

f. IACO registrars will—

(1) Report all incidents involving false information or manipulation of the IACS to MP officials.

(2) Develop a system to conduct a reconciliation with each sponsoring organization every 6 months to ensure the IACS database accurately shows the individuals the sponsoring organization has identified as current.

(3) Take the following actions to ensure the security, accountability, and procurement of installation-pass material is maintained:

(a) The plain, white plastic cardstock does not require any special security or accountability procedures.

(b) IACO registrars will record the destruction of all installation passes on AE Form 190-16C and annotate the final disposition of passes in the IACS. This form is available at <https://www.aeaim.hqusareur.army.mil/library/for/index-aeef.shtm>.

(c) IACOs will receive installation-pass cardstock laminate and ribbons from the USAREUR PM. IACOs will keep an adequate stock of passes, laminate, and ribbons at all times.

37. REGISTRATION PROCEDURES FOR INSTALLATION-PASS APPLICANT

a. IACO registrars will process requests for installation passes as follows:

(1) Follow the procedures in paragraph 30c if the sponsoring official cannot accompany an applicant to the IACO. This will enable the applicant to enter the installation to obtain an installation pass.

(2) Verify that the sponsoring official is authorized to perform sponsoring-official duties by checking the sponsoring organization's designation of sponsoring official memorandum that is on file. The issuing official will reject any application signed by an unauthorized sponsoring official.

(3) Receive the application and supporting documents from the applicant and reject any application that does not include required documentation. It is critical to the success of the Installation Access Control Program that registrars check the supporting documentation to minimize the potential of high-risk individuals obtaining access to U.S Forces installations in the USAREUR AOR.

(4) Register the applicant in the IACS with the information provided in the application. For restrictions that are subject to the sponsoring official's written justification (for example, sign-in privileges, number of installations authorized), the registrar will clarify any justification that is insufficient as a quality-control check for the overall system. In particular, if "USAREUR-wide" access is requested, registrars will check to see whether a lower level of access would be more appropriate, such as "USAREUR-wide (Germany only)."

(5) Before giving the applicant the installation pass, ensure that the applicant signs and dates an installation-pass-holder Acknowledgement of Responsibilities memorandum (app E) and the Privacy Act statement (fig 3). The applicant should keep a copy of the memorandum. The Privacy Act statement is required only for U.S. citizens.

PRIVACY ACT STATEMENT

AUTHORITY: Public Law 106-246, Title 10 USC, DODD 8500.1, AR 25-2, and EO 9397.

PRINCIPAL PURPOSE: To control local access to DOD information or information-based systems, and to control the physical access to installations, buildings, and controlled spaces by using measurable physical or behavioral characteristics to maintain accountability for issuance and disposition of installation passes.

ROUTINE USES: None. The "Blanket Routine Uses" are set forth at the beginning of the Army's compilation of systems of records notices.

DISCLOSURE: Voluntary. Failure to provide the requested information may result in denial of access to DOD information-based systems, DOD facilities, or both.

By signing below, I acknowledge that I have read and understand the conditions set forth in the above Privacy Act statement.

_____	_____	_____
Printed Name	Signature	Date

Figure 3. Privacy Act Statement

A *Datenschutzerklärung/Privacy Act Statement* (German version with English translation) is at the end.

(6) File the completed application packet. A complete application packet will include the application (AE Form 190-16A), a copy of supporting documents, a copy of the background-check initiation and results, the original copy of the acknowledgement of responsibilities memorandum, the Print Summary Page from the IACS, the original signed installation pass holder consent form (AE Form 190-16E (when approved, this form will be available at <https://www.aeaim.hqusareur.army.mil/library/for/index-aef.shtm>)), and the signed Privacy Act statement (for U.S. citizens only). For Temporary Installation Pass holders receiving an Installation Pass, the issuing official will file the notification information with the original Temporary Installation Pass application packet.

b. Procedures for issuing an Installation Pass when an individual has a valid Temporary Installation Pass are in paragraph 31. Information on processing renewal applications, lost and stolen passes, extensions to Temporary Installation Passes, and unserviceable Installation Passes is in paragraphs 32 through 35.

38. REGISTRATION PROCEDURES FOR DOD ID-CARD HOLDER

To register a DOD ID-card holder, registrars will—

- a. Verify the DOD ID-card holder's requirement to be registered in the IACS.
- b. Register the DOD ID-card holder in the IACS.
- c. File the signed and dated Privacy Act statement (app E).

39. REGISTRATION PROCEDURES FOR IDENTI-KID

Parents may register children under the age of 10 who do not have a DOD ID card using Identi-Kid. The Identi-Kid kit provides a way to collect a current photograph, fingerprints, vital statistics, and contact information. This information would be used by parents and law-enforcement personnel to locate a lost, kidnapped, or missing child. IACO registrars will register children under the age of 10 without a DOD ID card as follows:

- a. Each child must present a signed and completed AE Form 190-16D (available at <https://www.aeaim.hqusareur.army.mil/library/for/index-aeform190-16d.htm>) to be registered in IACS.
- b. The parent or legal guardian need not be present during registration. No installation pass will be issued.

40. PROCESSING ACCESS ROSTERS

- a. Access-roster procedures are explained in paragraph 42.
- b. Access rosters will be processed through the servicing IACO unless an exception applies according to paragraph 42e(5).
- c. IACO registrars will—
 - (1) Ensure access rosters are prepared and processed according to paragraph 42.
 - (2) Use the access-roster module in the IACS to automate the access-roster system after the IACS is operational at the ACPs.

SECTION VI ACCESS PROCEDURES

41. SIGN-IN PROCEDURES

Sign-in procedures will provide access to U.S. Forces installations in the USAREUR AOR if an access roster is unnecessary and issuing an Installation Pass is impractical or not authorized.

a. Sign-In Privileges.

(1) DOD ID-card holders who are military members or 18 years old and older have sign-in privileges. If this privilege has been suspended, it will be shown only in the IACS, not on the DOD ID-card itself. If a DOD ID-card holder has sign-in privileges withdrawn, the only way a guard will know this is by checking the IACS at the ACP. DOD ID-card holders not registered in the IACS are not authorized sign-in privileges.

(2) With the exception of individuals in the NATO Member and Department of State and American Embassy Personnel categories, Installation-Pass holders will not be granted sign-in privileges unless the sponsoring organization justifies the need. This action will be done during the IACS registration process. Sign-in privileges will be indicated on the front of all Installation Passes with any qualifications (for example, "contractors and vendors only") listed in the remarks block on the back. The Installation-Pass holder must be at least 18 years old. Temporary Installation Pass holders will not be authorized sign-in privileges.

b. Restrictions.

(1) Individuals under 18 years of age are not authorized sign-in privileges.

(2) Both DOD ID-card holders and Installation-Pass holders who are authorized sign-in privileges are limited to signing in four individuals and their vehicles at any one time. Using multiple sign-ins to circumvent this limit is prohibited.

(3) Individuals who require recurring access will not use sign-in procedures to avoid the installation-pass application process or access-roster requirements.

c. FPCON Restrictions. During FPCON Delta, only DOD ID-card holders will be authorized sign-in privileges.

d. Identification.

(1) Individuals who are signed in must show the guard their passport or personal ID (for example, German *Personalausweis*, Belgian Identity Card, Italian *carta d'identita*). Guards will ensure through visual comparison that the passport or personal ID belongs to the person being signed in.

(2) If the ACP is equipped with the IACS, guards will—

(a) Open the sign-in module and scan the DOD ID card or Installation Pass of the individual exercising his or her sign-in privileges. The IACS will automatically display a warning message if this individual is not authorized sign-in privileges and will not allow other data to be entered.

(b) Enter the names of the individuals being signed in up to the authorized limits (b(2) above). The IACS will automatically check the bar roster to ensure these individuals are not barred from the installation.

(3) If the ACP is not equipped with the IACS, the local SOP will provide procedures for accounting for signed-in individuals. The SOP for sign-in procedures should be as similar to those in (2) above as possible.

e. Sponsor Responsibilities. The sponsor will monitor the activity of individuals they sign in and be responsible for their conduct. Failure to follow sign-in policy and procedures may result in the withdrawal of sign-in privileges.

42. ACCESS ROSTERS

a. Access rosters will be used to provide access to installations if sign-in procedures and issuing an Installation Pass are impractical or unauthorized.

b. Permanent access rosters are not authorized. Access rosters will be temporary and will not be used to circumvent the installation-pass process. The maximum time an access roster may remain valid is 60 days.

c. Access rosters will be used for events that are nonrecurring and not regularly scheduled, are generally site-specific, and are coordinated in advance.

d. The following are examples of when access rosters should and should not be used:

(1) Example 1: An authorized DOD ID-card holder requires four meetings with several LNs (not already associated with the U.S. Armed Forces) over a 3-week period to discuss a project affecting the host nation. An access roster would be appropriate because the meetings are not regularly scheduled, are site-specific, and are not scheduled beyond 60 days.

(2) Example 2: A sanctioned private organization (for example, dance club) meets every Wednesday evening at 1900 and several of the members are LN employees. An access roster is not appropriate because the meetings are a recurring event. The participants must be signed in each week or issued an Installation Pass based on the Member of Private Organization category (para 22).

(3) Example 3: The directorate of public works hires a contractor to perform construction work on an installation for 2 weeks. An access roster is appropriate because the contract is for only 2 weeks and is site-specific.

(4) Example 4: A DOD ID-card holder wants to host a surprise birthday party at a morale, welfare, and recreation facility and the guestlist includes 10 people who have no means of access. An access roster is appropriate because the party is a single event and site-specific.

e. The following procedures must be conducted to process access rosters:

(1) Only DOD ID-card holders registered in the IACS may sign an access-roster request. IACO registrars will check the IACS to ensure the requester is a registered DOD ID-card holder.

(2) Original access-roster requests will be hand-carried to the servicing IACO or sent from a *.mil*, *.gov*, or *.org* e-mail address that includes the name of the individual signing the access-roster request (for example, john.smith@us.army.mil). If the request is sent by e-mail, the IACO issuing official will confirm receipt. Access-roster requests may not be sent by fax. A complete list of IACOs is at <http://www.hqusareur.army.mil/opm/iacs/Resources/USAREURIAACSRegistrationStations.pdf>.

(3) Access-roster requests will be submitted no less than 3 duty days before the desired effective date of the access roster to ensure IACO registrars have enough time to process the access roster.

(4) Access rosters will include the following information:

(a) Full name, country of citizenship, passport number or personal ID number (the number from one of the documents listed in para 30d(1), which must be shown to the guard before access is granted), and vehicle license-plate number, if applicable, of each individual.

(b) An effective date and expiration date, which may not be more than 60 days apart.

(c) The reason for the request, the location of the event or work to be performed, and the ACPs to which the access roster applies. For large-scale access-roster requests, such as one required to support the USAREUR Personal Property Shipment Program, the use of statements such as “USAREUR-wide” or “98th ASG-wide” is authorized. However, liberal access authorization like this should be avoided unless needed for operational requirements. The Installation Access Control Program limits access to the minimum number of installations to which access is required. Organizations will not use access rosters to circumvent the requirement to keep access to the absolute minimum simply for convenience.

(d) If the access roster is used to support a contractor or delivery service, include the company’s name and telephone number.

(e) If the access roster is being used to support delivery services, include the days and times when deliveries may be made (for example, Mondays 0700 to 1600).

(f) If an access roster is used for contract workers or vendors (for example, construction crew, contracted delivery services), a PGCC will be required and rules concerning residence and work permit requirements will apply. This documentation must accompany the access-roster request. If the request is sent by e-mail, the requester must indicate that the certificate has been received and permit requirements have been met.

(5) If an access roster is limited to one installation, the BSB may allow the access roster to be processed through designated individuals representing that installation (for example, the installation coordinator). BSBs will ensure these procedures are in local SOPs and special orders for ACP guards.

(6) BSBs will establish procedures to ensure—

(a) Individuals on access-roster requests are screened against the bar rosters and their country of citizenship is checked to ensure that any residence- and work-permit requirement is met.

(b) Access rosters are clearly marked to indicate they have been approved by the BSB before distribution.

(c) Approved access rosters are posted at applicable ACPs before the effective date.

f. The following procedures will be conducted by access-control guards:

(1) When an individual arrives at an ACP and informs the guard that he or she is on an access roster, the guard will obtain the passport or personal ID card (must be one of the documents listed in para 30d(1)) and compare the number on this document with the number on the access roster. These numbers must match.

(2) Guards will deny access when the individual is not on the access roster, information on the passport or personal ID card is not consistent with the information on the access roster, or the access roster has expired.

(3) If the access roster is being used to support delivery requirements, guards will check delivery paperwork to ensure the delivery location is identified.

(4) When access is authorized, guards will search the individual, bags, and vehicles according to the local SOP.

g. When the IACS is operational at BSB ACPs, the BSB will use the access-roster module in the IACS to process access rosters.

(1) IACO registrars will enter the access-roster information into the IACS and keep a printed copy of the access-roster request for distribution as needed.

(2) Guards will follow the procedures in subparagraph f above, except that they will conduct a manual look-up in the IACS instead of using a printed access roster.

43. EMERGENCY-VEHICLE AND PROTECTIVE-SERVICES-VEHICLE ACCESS

BSBs will use the following access procedures for emergency personnel and vehicles (for example, police, fire, ambulance, protective-services vehicles):

a. Access During Emergency Conditions.

(1) Plainly marked emergency vehicles (both U.S. and host-nation) with sirens on and lights flashing will not be unduly delayed, but occupants must still produce valid identification and the vehicle must be given at least an expedient search before being allowed to enter the installation.

(2) BSB commanders will coordinate with local host-nation emergency-service providers to establish notification procedures to use in case of an emergency. These procedures will include designation of ACP for entry, notification by emergency-service providers to the PMO, and PMO notification to ACPs of incoming emergency responders.

(3) BSBs will require emergency vehicles to come to a stop to allow guards an opportunity to identify the driver and occupants of the emergency vehicle, conduct an expedient inspection of the interior of the vehicle, and determine the location of the emergency. An "expedient search" will include a quick inspection of the passenger compartment and the rear cargo compartment or trunk of the vehicle.

NOTE: This stop should be conducted as quickly as possible (normally less than 30 seconds) and should be coordinated with emergency-service providers in advance to ensure providers understand the BSB access-control requirements under emergency conditions. PMOs will provide an escort for emergency responders observing the maximum stop time for these vehicles is 30 seconds.

b. U.S. Forces Police. U.S. Forces police (MP, USAFE security forces) in marked MP vehicles and wearing a military uniform are required to show ID. U.S. Forces police in civilian clothes (for example, MP investigators, Criminal Investigation Division agents) or in an unmarked vehicle will present proper ID and follow normal access-control procedures unless operating under emergency conditions.

c. Host-Nation Police.

(1) Host-nation police in marked police vehicles and wearing host-nation police uniforms are required to show ID when entering U.S. installations.

(2) Procedures in subparagraph a above will be used for host-nation police operating under emergency conditions.

(3) When the circumstances in (1) above do not apply, host-nation police will be required to show some type of personal ID (for example, passport, *Personalausweis*, German *Polizeausweis*, which has a name and picture on it and one of the following titles on the front: *Polizei Dienstausweis* (regular police); *Zoll-Polizei Dienstausweis* (customs police); *Kriminal-Polizei Dienstausweis* (criminal police)). The 22d ASG and 80th ASG should include a description of the host-nation police IDs in local SOPs. If there is any reason to doubt the validity of the ID or the reason for entry into the installation, the guard will call the servicing U.S. Forces police (for example, MP).

(4) Host-nation police who work on the installation with the U.S. Forces police may be issued an Installation Pass using the Official Guest category (para 25) to access the installation.

d. Fire Department Personnel. Fire department personnel who work for the U.S. Forces should be issued an Installation Pass using the Local National Employee category (para 13). Personnel from host-nation fire departments should enter U.S. Forces installations only during emergencies.

e. Ambulance Service Personnel. Ambulance service is provided by host-nation hospitals. Ambulances will normally enter installations under emergency conditions with the siren on and lights flashing. Ambulances will not be unduly delayed during an emergency (a above). Ambulances in Germany are well marked with some or all of the following words: Ambulance, *Krankenwagen*, or *Notarzt*. The 22d ASG and 80th ASG should include a description of the host-nation ambulances in their local SOPs.

f. Other Host-Nation Providers. BSBs should develop alternate access-control procedures for other host-nation service providers that respond to emergency situations that are not life-threatening (for example, water-, electric-, and heating-service providers). In these situations, unimpeded access should not be granted. BSBs should develop memorandums of agreement that require these service providers to notify the installation ahead of time when access will be required.

g. Protective-Services Vehicles.

(1) Protective-services heavy armored vehicles (HAVs) (commonly called “hard cars”) and security-escort vehicles (SEVs) (commonly called “chase cars”) do not have blanket authority to enter closed installations without presenting proper credentials.

(2) If ACP guards recognize the HAV and driver, they may choose not to stop the HAV and wave the vehicle and its occupants through the gate.

(3) Only HAV drivers will present their DOD ID card (no dispatch, license, or other documents). Exceptions to this requirement will be on an installation basis and approved by the ASG commander. The other occupants in HAVs will not be asked to provide ID.

(4) Guards will request that only the driver’s window be opened to receive the driver’s ID card. The guards will not look inside the vehicle, request the occupants to exit the vehicle, or attempt to search the vehicle.

(5) If an SEV is present, only the ID card of the first (lead) HAV driver will be checked. The lead HAV driver will inform the guards that the next vehicle is an SEV. The objective is to get these vehicles through the gate as quickly as possible without bypassing prudent security procedures.

NOTE: BSB commanders may establish alternate procedures or modify these procedures based on the FPCON.

44. ACP GUARDS

a. ACP guards will—

(1) Perform their duties according to this regulation and AE Regulation 190-13.

(2) Grant access only to individuals authorized access according to the policy and procedures in this regulation. Access authorization must be verified for all individuals entering a U.S. Forces-controlled installation, including all passengers in a vehicle (not just the driver).

(3) Follow the sign-in policy and procedures in paragraph 41 and the access-roster policy and procedures in paragraph 42.

(4) Notify MP officials if a DOD ID card or installation pass is expired or unserviceable. Guards may grant access to individuals who had their unserviceable DOD ID card or installation pass confiscated if the individual is registered in the IACS and is authorized access (g and h below). If the individual cannot be identified in the IACS, access will be denied unless an individual with sign-in privileges signs for the individual whose card or pass has been confiscated.

NOTE: All personnel conducting access control may confiscate DOD ID cards or installation passes using AE Form 190-16B. In accordance with paragraph 5g(1)(b), the BSB will establish receipt procedures for individuals whose cards or passes are confiscated and procedures to ensure these documents are turned in to the servicing IACO or ID-card-issuing facility as appropriate. A receipt for confiscated or expired DOD ID cards or installation passes will never be used as an authorized access document.

b. If the IACS is unavailable for access verification, guards must be able to manually check access documents. A second form of ID and a vehicle registration may be required based on local policy (for example, thoroughly checking personnel and vehicles during a specific FPCON or random antiterrorism measure). BSBs will include procedures for manually checking access documents in BSB policy and SOPs.

c. When the IACS is operational at an ACP, guards will scan 100 percent of DOD ID cards and installation passes unless operational requirements temporarily force the use of manual procedures to augment the IACS. This will provide positive verification of access authorization for individuals carrying these access documents. Checking other documents (for example, a second form of ID or vehicle registration) is not necessary if the individual is registered in the IACS and access is authorized.

NOTE: The full potential of IACS can only be realized with consistent and complete use of the system.

d. If scanning reveals that an installation-pass holder is not registered in the IACS, guards should check the date of issue. Same-day issues might not be in the IACS database. Local SOPs should provide procedures for granting access to individuals with an installation pass who may not be registered in the IACS. If, however, the date of issue is more than 1 day old, guards must coordinate with the servicing MP office. The servicing MP office will confiscate the installation pass and determine its validity.

e. Unless authorized by the BSB commander or higher authority, guards will not deny access to valid DOD ID-card holders who are not registered in the IACS. These individuals are normally on TDY, on temporary additional duty orders, or are new arrivals. Guards also will—

(1) Inform nonregistered DOD ID-card holders to register in the IACS as soon as possible.

(2) Log the entry of nonregistered DOD ID-card holders in the IACS to record their access. This requirement may cause a minor inconvenience for the DOD ID-card holder, which will encourage the cardholder to get registered in the IACS at the earliest opportunity. DOD ID-card holders requiring access to a U.S. Forces installation only for a short period (for example, a weekend softball tournament) normally will not be required to register in the IACS. If a DOD ID-card holder has registered in the IACS but the IACS database has not been updated, guards will treat the individual as a non-registered DOD ID-card holder.

(3) Check other ID documents (for example, a second form of ID or vehicle registration) according to local policy and SOPs.

NOTE: DOD ID-card holders not registered in the IACS are not authorized sign-in privileges.

f. BSB commanders will ensure special guard orders prescribe the procedures in subparagraph e above.

g. If a DOD ID card or installation pass will not scan properly in the IACS (for example, defective barcode) and the card or pass holder says that he or she is registered in the IACS, guards may verify registration by conducting a records search at the IACS workstation in the guard shack. DOD ID-card holders and installation-pass holders who are positively registered in the IACS will be granted access and instructed to immediately obtain a new DOD ID card or installation pass. When the record search reveals that the individual is not registered in the IACS, or the cardholder acknowledges that he or she is not registered in the IACS, guards will refer to subparagraph d above for installation-pass holders and subparagraph e above for DOD ID-card holders.

h. If a DOD ID-card holder or installation pass holder has forgotten his or her card or pass, BSB commanders may authorize guards to use the IACS manual look-up feature to authorize access as an alternative to denying access.

i. Employment as a contract security guard is not a basis for obtaining an installation pass. Contract guards will—

(1) Use sign-in procedures or access rosters when access is required on a nonrecurring basis (for example, to participate in training).

(2) Apply for an installation pass using the Contractor (Living in Host Nation) category (para 15) if access on a recurring basis is required because of the individual's position or duty location.

(3) Register in the IACS to support the user-logon requirements of the IACS during guard duty at ACPs with an operational IACS. A guard must obtain an installation pass in the Gate Guard category (para 29) to register in the IACS to perform user-logon requirements.

APPENDIX A REFERENCES

SECTION I PUBLICATIONS

Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons

Public Law 106-246, Military Construction Appropriations Act, 2001

Privacy Act of 1974

5 USC 552a(b), Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings

10 USC 3013, Secretary of the Army

10 USC 5013, Secretary of the Navy

10 USC 8013, Secretary of the Air Force

NATO Status of Forces Agreement Supplementary Agreement

DOD Directive 8500.1, Information Assurance (IA)

AR 25-2, Information Assurance

AR 190-13, The Army Physical Security Program

AR 190-56, The Army Civilian Police and Security Guard Program

AR 381-45, Investigative Records Repository

AR 600-8-14, Identification Cards for Members of the Uniformed Services, Their Family Members, and Other Eligible Personnel

Technical Manual 5-853-2, Security Engineering Concept Design

AE Regulation 190-1, Registering and Operating Privately Owned Motor Vehicles in Germany

AE Regulation 190-13, Army in Europe Physical Security Program

AE Regulation 525-13, Antiterrorism

USAREUR Regulation 600-700, Identification Cards and Individual Logistic Support

USAREUR Regulation 604-1, Foreign National Screening Program (Laredo Leader)

USAREUR Regulation 690-64, Local National Employee Conduct, Discipline, Complaints, Grievances, and Labor Disputes

SECTION II FORMS

SF 50-B, Notification of Personnel Action

DD Form 2(ACT), Armed Forces of the United States Geneva Convention Identification Card (Active)

DD Form 2(RET), United States Uniformed Services Identification Card (Retired)

DD Form 2(RES), Armed Forces of the United States Geneva Convention Identification Card (Reserve)

DD Form 2(RES RET), Armed Forces of the United States Identification Card (Reserve Retired)

DD Form 1172, Application for Uniformed Services Identification Card—DEERS

DD Form 1173, United States Uniform Services Identification and Privilege Card (Dependent)

DD Form 1173-1, United States Uniformed Services Identification and Privilege Card (Reserve Dependent)

DD Form 1934, Geneva Convention Identity Card for Medical and Religious Personnel Who Serve in or Accompany the Armed Forces

DD Form 2765, Department of Defense/Uniformed Services Identification and Privilege Card

DA Form 31, Request and Authority for Leave

DA Form 2028, Recommended Changes to Publications and Blank Forms

DA Form 3434, Notification of Personnel Action - Nonappropriated Funds Employee

AE Form 190-16A, Application for USAREUR/USAFE Installation Pass

AE Form 190-16B, Receipt for Confiscated ID Card

AE Form 190-16C, Record of Destruction

AE Form 190-16D, Identi-Kid Permission Slip IACS

AE Form 190-16E, IACS Installation Pass Holder Consent Form

AE Form 600-700A, USAREUR Privilege and Identification Card

AE Form 604-1B, Personnel Data Worksheet

**APPENDIX B
 FORMAT FOR DESIGNATION OF SPONSORING OFFICIALS MEMORANDUM**

Appropriate Letterhead

Office Symbol

Date

MEMORANDUM FOR *(enter the name of the servicing IACO)*

SUBJECT: Designation of Sponsoring Officials

1. The following individuals are designated as sponsoring officials for *(enter the name of the organization)*:

a. Authorized to grant up to U.S. Forces-wide access *(minimum LTC/GS-13/C-8/NF 5)*

FULL NAME	POSITION	GRADE	OFFICIAL E-MAIL ADDRESS
-----------	----------	-------	-------------------------

b. Authorized to grant up to ASG-wide access *(minimum SGM/CSM/MAJ/CW4/GS-12/C-7A/NF 4)*:

FULL NAME	POSITION	GRADE	OFFICIAL E-MAIL ADDRESS
-----------	----------	-------	-------------------------

c. Authorized to grant up to BSB-wide access *(minimum ISG/MSG/CW3/CPT/GS-11/C-7/NF 4)*:

FULL NAME	POSITION	GRADE	OFFICIAL E-MAIL ADDRESS
-----------	----------	-------	-------------------------

d. Authorized to grant access for only one installation *(minimum SFC/CW2/GS-9/C-6A)*:

FULL NAME	POSITION	GRADE	OFFICIAL E-MAIL ADDRESS
-----------	----------	-------	-------------------------

2. The POC for this information is *(include name, telephone number, and e-mail address)*.

Signature block of commander or designated official
(commander or first LTC/GS-13 in the chain of command)

APPENDIX C
SAMPLE AE FORM 190-16A

APPLICATION FOR USAREUR/USAFE INSTALLATION PASS (AE Reg 190-16)						
<p align="center">Data required by the Privacy Act of 1974</p> <p>Authority: Article 53, Supplementary Agreement to NATO SOFA; 10 USC 3012. Principal purpose(s): For identification of U.S. and non-U.S. nationals employed by U.S. Government agencies, contractors, and vendors of non-military agencies of countries in which U.S. personnel have been accommodated when these personnel require recurring access to the accommodations under U.S. control and do not possess other valid entry authorization documents. Routine use(s): To identify personnel authorized routine or recurring access to installations under U.S. control. Mandatory or voluntary disclosure and effect on individual not providing information: Voluntary. However, failure to provide any item of information will result in denial of entry onto the U.S.-controlled installations for which the AE Form 190-16A has been validated.</p>						
<p align="center">Please refer to the instructions on page 3 to ensure that the form is correctly filled in.</p>						
1. To 293d BSB, IACO Mannheim		2. From 5th Signal Command, Mannheim		3. Date (mm/dd/yyyy) 12/01/2004		
4. Applicant name (Last, first, MI) SCHMIDT, HANS L.		5. Sponsor address 5th Sig Cmd (NETC-SOP) CMR 420 APO AE 09056-0420		6. Address (Company/Organization/Unit) 5th Sig Cmd (NETC-SOP) CMR 420 APO AE 09056-0420		
7. Person category Local National Employee		8. Country of citizenship Germany		9. SSN/Personal ID number 6475611633		
10. Supporting document expiration date (Passport/ID card) (mm/dd/yyyy) 01/15/2006		11. Residence permit <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No		12. Work permit <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No		
13. Type pass requested <input checked="" type="checkbox"/> Installation pass <input type="checkbox"/> Temporary installation pass	14. Date of birth (mm/dd/yyyy) 11/17/1964	15. Weight (Pounds) 170	16. Height (Inches) 71	17. Eye (Color) Blue	18. Hair (Color) Brown	
19. Installations for which access is required USAREUR-wide (Germany only)						
20. Limitations/time/day access is required 24/7		21. FPCON restriction DELTA		22. Pass expiration date (mm/dd/yyyy) 01/15/2006 IACO REGISTRAR MUST VALIDATE		23. Sign-in privileges <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
24. Privately owned vehicle (POV) registration information (additional vehicles may be added on a separate sheet of paper)						
a. License number	b. Country	c. Make	d. Model	e. Year	f. Body type	g. Color
MA-T123	Germany	Ford	Ka	2003	2-door	White
25. Company name and telephone number						
26. Verification by sponsoring official (must check both boxes)						
<input checked="" type="checkbox"/> I have reviewed the results of all background checks required by AE Reg 190-16 and verify that there is no derogatory information that would preclude the issuing of an installation pass.						
<input checked="" type="checkbox"/> I verify that the applicant has been informed about the purpose and proper use of the installation pass. I have reviewed AE Reg 190-16 and believe this packet is administratively correct, and fully and accurately reflects the applicant's access requirements. However, if there is a problem or you need further information please contact me.						
a. Organization and telephone number 5th Signal Command DSN 381-9303			b. Name and title COL Bill B. Brown, G-3			
c. Signature			d. Date (mm/dd/yyyy)			
27. To be completed by registrar						
a. Registrar name			b. Date issued			

28. Installation for which access is required (Provide justification)

Mr. Schmidt's job involves conducting network infrastructure surveys in support of all the signal battalions in Germany. This requires him to travel to all the ASGs in Germany, hence USAREUR-wide access (Germany only) is required.

29. Sign-in privileges (Provide justification)

While conducting network infrastructure surveys, Mr. Schmidt must coordinate with and involve host nation telecommunications experts to ensure that DOD does not violate host nation laws and statutes. This requirement necessitates that Mr. Schmidt be able to sign on these people to accomplish his mission.

Required attachments (Check applicable boxes)

Requirements may be different depending on the person category selected. All installation-pass applications must include supporting documents. Some installation-pass applications may include a copy of:

- | | |
|--|--|
| <input type="checkbox"/> Residence permit | <input type="checkbox"/> Defense Clearance Investigation Index (DCII) |
| <input type="checkbox"/> Work permit | <input checked="" type="checkbox"/> Proof of AE Form 604-1A, Foreign National Screening (FNS), initiation/completion |
| <input checked="" type="checkbox"/> Police Good Conduct Certificate (PGCC)
(<i>Polizeiliches Führungszeugnis</i>) | <input checked="" type="checkbox"/> Military police (MP) check results |

Instructions for completing AE Form 190-16A

Item 1. To

Enter the name of the servicing installation access control office.

Item 2. From

Enter the name of the sponsoring official's organization.

Item 5. Sponsor address

Enter the mailing address of the sponsoring organization. For the person categories Personal-Service Employee, Visitor (immediate family member living in Europe), and Visitor (friend or family member not included in the "immediate family member living in Europe)" category, also include the requester's mailing address.

Item 6. Address

Enter the address of the unit of assignment. This address will depend on the applicant's person category. For example, for local national employees, enter the hiring organization's address. For Contractors and Delivery Personnel, enter the address of their company. Visitors should list their home mailing address.

Item 7. Person category

- DOD ID-card holder
- Local national employee
- Contractor (based in United States)
- Contractor (living in host nation)
- Personal-service employee
- Delivery personnel (recurring deliveries or similar service not associated with a Government contract)
- Vendor or commercial solicitor
- NATO member
- Host-nation military member
- Foreign student (Marshall Center)
- Member of private organization
- Visitor (immediate family member living in Europe)
- Visitor (friend or family member not included in category above)
- Official guest
- Department of State and American Embassy personnel
- Other
- Host-nation Government official
- Gate guard

Item 9. SSN/Personal ID number

Enter the personal ID number or the passport number from the supporting document used. Applicant must have one of the following supporting documents:

- Passport
- Personal ID card issued by the country of citizenship (for example, German *Personalausweis*, Belgian identity card, Italian *carta d'identità*)
- Military ID card issued by one of the NATO Sending States (Belgium, Canada, France, the Netherlands, United Kingdom)

Item 10. Supporting document expiration date

Enter the expiration date of the supporting document (for example, expiration date of passport or German *Personalausweis*).

Item 11. Residence permit

If required, check the appropriate box to indicate whether a copy of the residence permit is attached. See AE Reg 190-16 for guidance.

Item 12. Work permit

If required, check the appropriate box to indicate whether a copy of the work permit is attached. See AE Reg 190-16 for guidance.

Item 13. Type pass requested

Check the appropriate box. If an installation pass is desired, a temporary installation pass may be issued pending completion of a required background check. A temporary installation pass is valid for up to 90 days. The restrictions associated with each pass are different for each individual's access requirements.

Item 19. Installations for which access is required

Enter the level of access required. Depending on the person category, access may be restricted per AE Reg 190-16. Access should be limited to the least amount required. Examples include Taylor Barracks; 293d BSB (Mannheim); 26th ASG-wide; USAREUR-wide (Germany only).

The following levels of USAREUR-wide access are available:

- USAREUR/USAFE-wide
- USAREUR-wide
- USAREUR/USAFE (Germany only)
- USAREUR (Germany only)

NOTE: If liberal access is required, the sponsoring organization and the IACS registrar must take steps to ensure the proper selection from the above is made. For example, a contractor who operates exclusively within Germany should never be given USAREUR/USAFE-wide access.

Item 19. Installations for which access is required (continued)

If any level of USAREUR-wide access is requested above, the sponsoring official must include a written justification in item 27. The written justification must demonstrate why the applicant requires the level of access in the performance of duties. NATO Member and Department of State and American Embassy person categories are defaulted to USAREUR/USAFE-wide access; no justification is required.

Item 20. Limitations/time/day access is required

Enter "24/7" if access is required all the time; otherwise state the specific days of the week and times. IACOs may require justification for liberal access (such as 24/7), so sponsoring organizations should be prepared to justify this entry.

Item 21. FPCON restriction

Enter the FPCON restriction. The IACS will establish a default FPCON according to AE Reg 190-16. Sponsoring officials may request a reduction or a one-FPCON increase.

- Delta
- Charlie
- Bravo
- Alpha

Item 22. Pass expiration date

Enter the desired installation pass expiration date. This field will be validated by the IACO. Justification for this date must be provided. A temporary installation pass is valid for up to 90 days. The expiration date of an installation pass depends on the limitations of the person category (item 7) selected as well as the expiration date of the supporting document (for example, passport) that was used to obtain the installation pass. The expiration date will be whichever date is earlier.

Item 23. Sign-in privileges

Check the appropriate box to indicate whether sign-in privileges are required. If sign-in privileges are requested, the sponsoring official must include a written justification in item 28. The written justification must demonstrate why the applicant requires sign-in privileges in the performance of duties. NATO Member and Department of State and American Embassy person categories are defaulted to sign-in privileges authorized; no justification is required.

Item 24. Privately owned vehicle (POV) registration information

- a. State the license plate number exactly as it appears.
- b. State the country the license plate was issued for.
- c. State the make of the vehicle (for example, Opel, Saab, BMW).
- d. State the model of the vehicle (for example, 325i, Astra, 190E, S60).
- e. State the year of the vehicle (YYYY).
- f. State the body type of the vehicle (for example, 2-door sedan, bus).
- g. State the color of the vehicle.

Item 25. Company name and telephone number

This item is only applicable for applicants in the Contractor (living in host nation) person category. If applicable, enter the name and telephone number of the company.

Item 26. Verification by sponsoring official authority

State the name, title, organization, and telephone number of the sponsoring official. The BSB IACO must have a copy of the designation of sponsoring officials memorandum from your organization identifying who is authorized to sign installation pass applications.

Item 27. To be completed by registrar.

Item 28. Installations for which access is required

Enter the written justification that demonstrates why the applicant requires the level of access in the performance of duties.

Item 29. Sign-in privileges

Enter the written justification that demonstrates why the applicant requires sign-in privileges in the performance of duties.

**APPENDIX D
HEIGHT AND WEIGHT CONVERSION CHARTS**

**Weight-Conversion Chart:
(2.2045 pounds = 1 kg)**

Weight in kilograms	Converted to pounds
35	77
37	82
39	86
41	90
43	95
45	99
47	104
49	108
51	112
53	117
55	121
57	126
59	130
61	134
63	139
65	143
67	148
69	152
71	157
73	161
75	165
77	170
79	174
81	179
83	183
85	187
87	192
89	196
91	201
93	205
95	209
97	214
99	218
101	223
103	227
105	231
107	236
109	240
111	245
113	249
115	254
117	258
119	262
121	267
123	271
125	276
127	280
129	284
131	289
133	293
135	298
137	302

**Height-Conversion Chart
(.39370 inches = 1 cm)**

Height in centimeters	Height in feet and inches	Height in inches
122	4 feet 0 inches	48
124	4 feet 1 inches	49
127	4 feet 2 inches	50
130	4 feet 3 inches	51
132	4 feet 4 inches	52
135	4 feet 5 inches	53
137	4 feet 6 inches	54
140	4 feet 7 inches	55
142	4 feet 8 inches	56
145	4 feet 9 inches	57
147	4 feet 10 inches	58
150	4 feet 11 inches	59
152	5 feet 0 inches	60
155	5 feet 1 inches	61
157	5 feet 2 inches	62
160	5 feet 3 inches	63
163	5 feet 4 inches	64
165	5 feet 5 inches	65
168	5 feet 6 inches	66
170	5 feet 7 inches	67
173	5 feet 8 inches	68
175	5 feet 9 inches	69
178	5 feet 10 inches	70
180	5 feet 11 inches	71
183	6 feet 0 inches	72
185	6 feet 1 inches	73
188	6 feet 2 inches	74
191	6 feet 3 inches	75
193	6 feet 4 inches	76
196	6 feet 5 inches	77
198	6 feet 6 inches	78
201	6 feet 7 inches	79
203	6 feet 8 inches	80
206	6 feet 9 inches	81
208	6 feet 10 inches	82
211	6 feet 11 inches	83

APPENDIX E
SAMPLE INSTALLATION-PASS-HOLDER ACKNOWLEDGEMENT OF RESPONSIBILITIES

MEMORANDUM FOR RECORD	Date	
SUBJECT: Acknowledgement of Installation-Pass-Holder Responsibilities		
1. Reference AE Regulation 190-16, Installation-Access Control, 18 January 2005.		
2. As a USAREUR/USAFE Installation Pass holder, I acknowledge the following:		
a. All persons, their personal property, U.S. Government property, and vehicles may be searched on entry, while within the confines of, or when leaving U.S. Forces installations. Persons attempting to gain entry who refuse to identify themselves, provide digitized fingerprint minutia data (DFMD), or consent to search will be denied access.		
b. If I am authorized sign-in privileges, I understand that at no time will I have more than four persons and their vehicles signed in. I understand that by signing for another person to enter a U.S. Forces installation, I am agreeing to monitor that person's actions at all times, and I accept full responsibility for that person's conduct. I will ensure that the signed-in person complies with U.S. Forces and local policy.		
c. Installation Passes are U.S. Government property. Any access-control person may confiscate an Installation Pass that has expired, is being used fraudulently, is being presented by a person other than the person to whom it was issued, or is obviously altered, damaged, or mutilated.		
d. I must surrender my pass when—		
(1) It is replaced (except when lost or stolen).		
(2) I no longer require access.		
(3) My sponsor-status changes.		
(4) I resign or retire, am terminated, or am no longer officially sponsored.		
e. If I lose my Installation Pass or if it is stolen, I must immediately notify either the MP or installation access-control office that issued the pass. Failure to do so is grounds for denying a replacement pass.		
f. Violations of U.S. Forces security policy may be grounds for denying access to U.S. Forces installations and lead to confiscation of installation-access documents.		
3. I acknowledge by my signature that I have read and understand the policy, requirements, and responsibilities above.		
_____	_____	_____
(Print) Last, First, MI	Signature	Date

GLOSSARY

SECTION I ABBREVIATIONS

1st PERSCOM	1st Personnel Command
AAFES-Eur	Army and Air Force Exchange Service, Europe
ACP	access-control point
AOR	area of responsibility
ASG	area support group
AST	area support team
BSB	base support battalion
CAC	Common Access Card
COR	contracting officer's representative
CPAC	civilian personnel advisory center
CPF	central processing facility
DCII	Defense Clearance and Investigation Index
DEERS	Defense Enrollment Eligibility Reporting System
DEROS	date eligible for return from overseas
DFMD	digitized fingerprint minutia data
DOD	Department of Defense
EU	European Union
FNS	foreign national screening
FPCON	force protection condition
G2	Deputy Chief of Staff, G2, USAREUR
HAV	heavy armored vehicle
IACO	installation access control office
IACS	Installation Access Control System
ID	identification
IMA-E	United States Army Installation Management Agency, Europe Region Office
JA	Judge Advocate, USAREUR
LN	local national
MIPR	military interdepartmental purchase request
MP	military police
NATO	North Atlantic Treaty Organization
NCO	noncommissioned officer
OCONUS	outside the continental United States
PCS	permanent change of station
PDA	personal digital assistant
PGCC	police good conduct certificate
PM	Provost Marshal, USAREUR
PMO	provost marshal office
POC	point of contact
POV	privately owned vehicle
PR&C	purchase request and commitment
SCOR	site contracting officer's representative
SEV	security-escort vehicle
SOFA	Status of Forces Agreement
SOP	standing operating procedure
TDY	temporary duty
TM	technical manual
U.S.	United States
USAFE	United States Air Forces in Europe
USAREUR	United States Army, Europe

SECTION II TERMS

access roster

One of four ways an individual can be granted access to U.S. Forces-controlled installations; an approved list of individuals authorized unescorted access to an installation.

applicant

An individual applying for an installation pass.

application

AE Form 190-16A used to apply for an installation pass.

category

Designation of individuals registered in the Installation Access Control System. There are 18 different categories. Each category has specific risk-based registration requirements and restrictions based on the relationship between the individual and the U.S. Forces. One category is for DOD ID-card holders; the remaining 17 categories are for installation-pass applicants.

contractor

An individual working under contract for DOD. This includes subcontractors (individuals contracted by the primary contractor to perform portions of a contract), primary contractors, and individual contractors.

controlled-access installation

A U.S. Forces installation where access is controlled by guards.

Foreign National Screening Program

A program managed by the USAREUR G2 that is designed to conduct background checks on non-U.S. citizens.

in loco parentis

In the position or place of a parent.

installation access control office

An office, normally at the base support battalion or area support team, that is authorized by the Provost Marshal, USAREUR, to register individuals into the Installation Access Control System and produce and issue installation passes.

Installation Access Control System

The personnel access-verification system that manages the Installation Access Control Program in the USAREUR area of responsibility.

logical access

The right to use installation-access verification systems (computers) with no right to physical access to the installation.

probable cause

Reasonable grounds for supporting that a charge is well-founded.

registrar

An official who is authorized to register individuals into the Installation Access Control System and issue installation passes. Registrars normally work at the installation access control office.

requester

A DOD identification-card holder who requests an installation pass for an individual, but is not authorized to perform sponsoring-organization responsibilities. The requester status applies only to the Personal-Service Employee (para 16) and the two Visitor (paras 23 and 24) categories of the Installation Access Control System.

sign-in

A privilege granted to certain categories of individuals that allows them to escort visitors after signing them on to an installation.

sponsoring official

An individual who represents the sponsoring organization and carries out the organization's sponsoring responsibilities. Sponsoring officials must be designated in writing.

sponsoring organization

The organization that performs installation-pass responsibilities based on the organization's relationship to the installation-pass applicant. Sponsoring organizations are identified for each category of applicant. Sponsoring organizations verify the legitimacy of the applicant's need to access U.S. Forces installations. Every installation-pass applicant and installation-pass holder has a sponsoring organization.

unserviceable

Any condition or change to a DOD identification card or installation pass that impairs the guard's ability to verify that the card or pass holder is the individual on the card or pass, or that causes the guard to question whether or not the card has been altered. "Unserviceable" does not include minor bends, peeled lamination, print fading, or other deficiencies that do not impair the guard's ability to verify that the card or pass holder is the individual indicated.

DATENSCHUTZERKLÄRUNG

Die Regierung der Vereinigten Staaten von Amerika sieht sich in besonderer Weise dem Schutz der Privatsphäre des Individuums verpflichtet. Als Teil der Executive achtet das US-Verteidigungsministerium auf den Schutz persönlicher Daten, die im Rahmen dienstlicher Belange von Mitarbeitern, Vertragsnehmern und dritten Personen erhoben werden müssen. Dabei wenden die Dienststellen des Verteidigungsministeriums im Ausland das jeweils einschlägige nationale Datenschutzrecht an.

Im Hinblick auf die Bedrohung durch den internationalen Terrorismus sind die Dienststellen der US Streitkräfte bemüht den grösstmöglichen Schutz von Personal, Gerätschaften und Liegenschaften vor Anschlägen sicherzustellen. Hierzu ist es erforderlich, den Zugang zu den Liegenschaften zu beschränken und sicherzustellen dass nur berechtigte Personen Zugang erhalten. Diesem Zweck dient die Einführung eines mit biometrischen Daten (digitalisiertes Lichtbild und zwei Fingerabdrücke) ausgestatteten Ausweises, der Installation Access System Control Card, der eine schnelle und sichere Personenidentitätsfeststellung ermöglicht.

Ihre mit dem Antragsformular 190-16A zu den Nummern 4-10,13-25 erhobenen persönlichen Daten werden in eine regionale Datenbank des Installation Access Systems (IACS) aufgenommen und gespeichert. Dies gilt auch für die digitalisierten Fingerabdrücke und das Lichtbild. Für die Datenbank ist das Office of the Provost Marshall verantwortlich.

Die Daten werden ausschliesslich zur Identitätsüberprüfung im Zusammenhang mit dem Zugang zu und dem Aufenthalt in Einrichtungen der US Streitkräfte verwendet. Sie werden durch Zugangskontrollsysteme entsprechend dem jeweiligen Stand der Technik gegen unberechtigten Zugriff geschützt und sind nur dem mit der Aufgabe des Liegenschaftsschutzes betrauten Personenkreis zugänglich. Durch die Lesegeräte wird über einen automatischen Abgleich der auf dem Ausweis verschlüsselt enthaltenen Daten mit der Datenbank die Echtheit des Ausweises überprüft.

Eine Übermittlung der Daten an Stellen ausserhalb der Bundesrepublik Deutschland erfolgt nicht. Mit dem Liegenschaftsschutz betraute Dienststellen des U.S.-Verteidigungsministeriums in Europa haben zu Zwecken der Personenzugangskontrolle Zugriff auf die gespeicherten Daten, wenn die betroffene Person eine in Europa ausgestellte Installation Access Control Card vorlegt. Eine Übermittlung von Daten an Dienststellen der Bundesrepublik Deutschland erfolgt nur soweit dies nach den rechtlichen Bestimmungen des Bundesdatenschutz-gesetzes zulässig ist.

Bei einem Ausscheiden aus dem Dienst bei den US Streitkräften bzw. bei Wegfall der Notwendigkeit, im Rahmen dienstlicher oder vertraglicher Belange Liegenschaften der US Streitkräfte zu betreten, werden die gespeicherten Daten in ein gesichertes Datenarchiv transferiert und dort nach einem Zeitraum von 5 Jahren vollends gelöscht.

Andere als die mit der Antragsstellung angeforderten persönlichen Daten werden nicht erhoben. Der Antragsteller ist befugt beim zuständigen IACS-Office unentgeltlich Auskunft über die über ihn gespeicherten Daten und gegebenenfalls deren Korrektur zu verlangen.

Die Hauptbetriebsvertretung der bei den US-Streitkräften beschäftigten Ortskräfte hat der Erhebung, Speicherung und Verwendung der persönlichen Daten im Zusammenhang mit der Einführung des neuen Liegenschaftszugangkontrollsystems zugestimmt.

Von der vorstehenden Datenschutzerklärung habe ich Kenntnis genommen. Mir ist bekannt, dass eine Verweigerung der Einwilligung zur Verweigerung des Zugangs zu den Liegenschaften führen kann. Dies kann – mit weiteren Folgen – dazu führen, dass ich meinen vertraglichen Verpflichtungen nicht nachkommen kann.

Ich stimme der Speicherung meiner Daten in der IACS Datenbank zu.

(Ort, Datum)

(Unterschrift)

Translation

PRIVACY ACT STATEMENT

The Government of the United States of America considers itself especially obligated to protect individual privacy. The Department of Defense (DoD), as part of the executive branch, attaches great importance to the protection of personal data, which have to be collected from employees, contractors and third parties within the scope of official requirements. DoD agencies abroad are complying also with the respective national data protection laws.

In view of the threat posed by international terrorism, US Forces agencies are attempting to provide maximum protection against terrorist attacks for personnel, equipment and accommodations. In order to achieve this, it is necessary to limit access to the accommodations and to ensure that authorized persons only have access. For this purpose, an ID-Card containing biometric data (digitized photo and two finger prints) - the Installation Access Control System Card was introduced, making a fast and certain personnel identification possible.

Your personal data collected on Application Form 190-16A under Item 4 to 10 and 13 to 25 will be stored in a regional data base of the Installation Access Control System (IACS). This also applies to the digitized finger prints and the photo. The Office of the Provost Marshal is responsible for the data base.

The data will be used exclusively for individual identification in connection with access to and presence on US Forces installations. The data will be protected against unauthorized access by state of the art access control systems and will be accessible only for the category of personnel responsible for installation protection. By applying the screening device in order to compare the encrypted data on the ID-cards to the data in the data base, the authenticity of the ID-card will be verified.

The data will not be transferred to agencies outside of the Federal Republic of Germany. This does not apply to the transfer of data to activities of the US Forces located in Europe for identification purposes in connection with granting access to installations of the US Forces in those countries. The recipient is not authorized to transfer the data any further. Data will be transferred to agencies of the Federal Republic of Germany only if permissible under the statutory provisions of the Federal Republic of Germany.

In the case of termination of employment with the US Forces, respectively, if access to the installations within the scope of official or contractual purposes is no longer required, the personal data will be transferred to a secure data archive and will be deleted entirely after 5 years.

Other data than those requested upon application will not be collected. The applicant is authorized to demand free-of-charge information from the responsible IACS Office concerning the data stored about him/her and, if applicable, may demand correction.

The Head Works Council of the Local Nation employees of the US Forces has consented to the collection, storage and utilization of personal data in connection with the introduction of the new Installation Access Control System.

I have taken notice of the above Privacy Act Statement. I am aware that my refusal to consent may result in denial of access to the installations. This may result – with further consequences - in my inability to comply with my obligations.

I consent to the storage of my data in the IACS data base.

(location, date)

(signature)

22. März 2005

Military Police

Kontrolle des Zugangs zu Einrichtungen

*Diese Dienstvorschrift ersetzt *AE Regulation 190-16-G* vom 19. Oktober 2003.

Diese Dienstvorschrift ist eine Übersetzung der *AE Regulation 190-16*. Die deutsche Fassung ist für alle Arbeitnehmer bindend, die nach den Bestimmungen des TV AL II beschäftigt werden.

For the CG, USAREUR/7A:

E. PEARSON
Colonel, GS
Deputy Chief of Staff

Official:



GARY C. MILLER
Regional Chief Information
Officer - Europe

Zusammenfassung. Diese Dienstvorschrift legt Richtlinien und Verfahren für die Kontrolle des Zugangs zu Einrichtungen der US-Streitkräfte fest. Die Dienstvorschrift gilt nicht für durch andere Dienstvorschriften geregelte Sicherheitsbereiche (*AR 190-13*).

Zusammenfassung der Änderungen. Diese überarbeitete Dienstvorschrift

- enthält als neue Personengruppen die Gruppe der „Vertreter von Regierungsstellen/Behörden des Aufnahmestaates“ sowie die der „Wachposten“ mit den entsprechenden Zugangsregelungen (Abs. 28 und 29);
- schreibt bindend die Verwendung von Formblatt *AE Form 190-16B, Receipt for Confiscated ID Card; AE Form 190-16C, Record of Destruction; AE Form 190-16D, IACS Identi-Kid Permission Slip*; sowie *AE Form 190-16E, IACS Installation Pass Holder Consent Form*;
- enthält neu: Verfahren zum Einzug von Kasernenausweisen und *DOD ID-Cards* von Personen, die nicht länger Zugang zu Einrichtungen benötigen bzw. im Besitz unbrauchbarer oder abgelaufener Kasernenausweise oder *DOD ID-Cards* sind;
- gewährt Inhabern eines gültigen Besucherausweises, die vorübergehend Zugang zu weiteren Einrichtungen als den auf ihrem Ausweis angegebenen benötigen, in Begleitung der den Zugang beantragenden Person diesen erweiterten Zugang;
- enthält neu: Verfahren zur Ausstellung von Kasernenausweisen an US-Zivilbedienstete, denen aufgrund der kürzlich vom US-Verteidigungsministerium verhängten Ausstellungssperre keine *Common Access Card (CAC)* ausgestellt werden kann (Abs. 9c);
- stellt klar, dass auf der Rückseite von *CAC-Cards*, die keinen Zugang zu militärischen Einrichtungen gewähren (wie sie in der Regel in den USA Zivilisten oder Mitarbeitern verpflichteter Privatfirmen ausgestellt werden), zwar keine *Social Security Number* angegeben ist, ihre Inhaber aber dennoch zum Zwecke der Registrierung im *IACS* wie Inhaber einer *DOD ID-Card* zu erfassen sind;

- weitet die Befugnis als *Sponsoring Organization* zu fungieren, wenn Zugang zu mehr als drei *Area Support Groups (ASG)* (regionale Unterstützungsgruppen) beantragt wird, auf zusätzliche Organisationen aus;
- stellt klar, dass personengruppenbedingte *Foreign National Screening (FNS)* Überprüfungen für nicht-amerikanische und amerikanische Angehörige dieser Gruppen vor Ausstellung eines Kasernenausweises durchzuführen sind, wenn diese seit mehr als 12 aufeinander folgenden Monaten in Deutschland leben;
- definiert folgende Gruppen neu: „Besucher (direkte Familienangehörige, in Europa lebend)“, „Besucher (Freunde, Bekannte oder Familienangehörige, die nicht unter vorstehende Personengruppe fallen)“ und „Offizielle Gäste“ (Abs. 23-25);
- enthält aktualisierte Vorgaben bzgl. der Gruppe der offiziellen Gäste (Abs. 25)
- enthält als neue Auflage für Antragsteller, die aufgrund der Zugehörigkeit zu einer bestimmten Personengruppe ein polizeiliches Führungszeugnis vorzulegen hätten, denen aber ein solches Zeugnis nicht ausgestellt werden kann (weil sie noch kein Jahr in Deutschland leben), die Vorlage eines entsprechenden Zeugnisses vom bisherigen Wohnsitzland. Dieses Zeugnis ist mit englischer Übersetzung vorzulegen;
- stellt klar, dass einigen nicht-deutschen Mitarbeitern von Privatfirmen, die als technische Sachverständige tätig sind, u. U. kein polizeiliches Führungszeugnis ausgestellt werden kann;
- stellt klar, dass für Personen, die als Geheimnisträger bereits sicherheitsmäßig überprüft wurden, eine Überprüfung auf der Grundlage des *Defense Clearance and Investigation Index (DCII)* nicht erforderlich ist;
- schreibt bindend vor, dass Personen, die im Rahmen des *FNS* überprüft werden, Formblatt *AE Form 604-1B* zu unterschreiben haben;
- enthält zusätzliche Vorgaben zur Minimierung der Sicherheitsrisiken für die *Base Support Battalions (BSBs)* (Standortunterstützungsverband).
- enthält bei einem Aufenthalt von mehr als 90 aufeinander folgenden Tagen in Deutschland als zusätzliche Auflage die Vorlage einer Aufenthaltserlaubnis;
- enthält als zusätzliche Auflage, die Vorlage einer Kopie der Beitrittsurkunde (bei Mitgliedschaft in einem Verein), des entsprechenden Dokuments (bei Ermächtigung, „in loco parentis“ zu handeln) bzw. von Formblatt *AE Form 600-700A* zur Begründung des Erfordernisses des Zugangs zu Einrichtungen;
- stellt klar, dass Personen, die der Gruppe der ortsansässigen Arbeitnehmer angehören (Abs. 13) und vor dem 3. Oktober 1985 eingestellt wurden, eine Überprüfung durch die US-Militärpolizei nicht nachzuweisen haben;
- stellt klar, dass ortsansässige Arbeitnehmer (Abs. 13) bei einem Dienststellenwechsel ohne Dienstunterbrechung ihren Status beibehalten. Ein neues polizeiliches Führungszeugnis und eine erneute Überprüfung durch die US-Militärpolizei sind deshalb nicht erforderlich;
- schreibt bindend vor, dass vor Ausstellung eines neuen Kasernenausweises der ablaufende bzw. abgelaufene Ausweis abzugeben ist. Falls dieser von Wachposten eingezogen wurde, ist Formblatt *AE Form 190-16B* als Einzugs-/Empfangsbestätigung vorzulegen;
- stellt klar, dass sich die für die Ausstellung zuständigen Mitarbeiter im *Installation Access Control Office (IACO)* mit dem *S-2* oder *Security Manager* in Verbindung zu setzen haben, um den Stand der *FNS*-Überprüfung zu ermitteln, wenn ausstehende *FNS*-Ergebnisse der Grund für den Antrag auf Verlängerung eines Ausweises sind;
- stellt klar, dass die Genehmigung für die erneute Verlängerung eines befristeten Kasernenausweises, der aufgrund ausstehender *FNS*-Ergebnisse bereits 90 Tage verlängert wurde (Gesamtgültigkeit somit 180 Tage), ausschließlich vom *USAREUR Provost Marshal (PM)* erteilt werden kann;
- weitet die Berechtigung, *DOD ID-Cards* bzw. Kasernenausweise einzuziehen, auf alle den Zugang kontrollierenden Personen aus. Formblatt *AE Form 190-16B* ist als Einzugs-/Empfangsbestätigung auszufüllen;
- schreibt bindend vor, dass *IACO*-Registatoren einen Nachweis über die Vernichtung von Kasernenausweisen zu führen, diese auf Formblatt *AE Form 190-16C* zu dokumentieren und im *Installation Access Control System (IACS)* zu erfassen haben;

- enthält zusätzliche Bestimmungen, nach denen *IACOs* vom *USAREUR PM* neben einem Vorrat an Blankoausweisen und Folienmaterial Drucker-Farbbänder erhalten, die jederzeit in angemessenem Umfang vorzuhalten sind;
- enthält zusätzliche Vorgaben bzgl. der bei der Antragstellung vorzulegenden Unterlagen. Neben dem Antrag (Formblatt *AE Form 190-16A*), einer Kopie der für die Antragstellung vorgelegten Dokumente, dem Originalschreiben bzgl. der Anerkennung der Pflichten eines Ausweisinhabers, dem Testausdruck aus dem *IACS*-Registrierungsmodul und der unterschriebenen Erklärung zum *Privacy Act* (gilt nur für US-Staatsangehörige) ist eine Kopie der Einleitung von Personenüberprüfungen sowie ihrer Ergebnisse vorzulegen;
- enthält Vorgaben bzgl. der datenmäßigen Erfassung von Kindern (Abs. 39);
- äßt als weitere E-Mail Adressen, über die Erstanträge auf Erstellung von Registrierungslisten gestellt werden können, außer die mit einer „mil“-Kennung auch solche mit der Kennung „gov“ oder „org“ zu;
- enthält als neue Ausdrücke im Glossar den Ausdruck „in loco parentis“ sowie den Ausdruck „logischer Zugang“;
- schreibt bindend vor, dass die ständigen Dienstanweisungen für Wachposten Vorgaben zu enthalten haben, wie nach Erscheinen der verschiedenen Anzeigen (z. B. Eintrag archiviert, Nicht registriert) auf dem Handscanner bzw. der an den Toren bereitgestellten Computer vorzugehen ist;
- enthält nähere Angaben zu *DD Form 2 (RES)*;
- entzieht dem *1st Personnel Command (1st PERSCOM)* die Befugnis als Sponsor für die Gruppe der Händler und Dienstleister zu fungieren und enthält keinen Verweis auf *1st PERSCOM* als Gewerbeschein-ausstellende Stelle mehr;
- enthält keinen Verweis auf bestimmte Kapitel von *USAREUR Regulation 600-700* mehr;
- stellt klar, dass Kommandeure befugt sind, Strafen gegen Personen zu verhängen, die gegen Bestimmungen bzgl. der Berechtigung zum Eintragen von Personen in Besucherlisten verstoßen;
- aktualisiert die Vorgaben bzgl. der Einfahrt von Einsatz- und Rettungsfahrzeugen sowie von Fahrzeugen des Personenschutzes;
- enthält als neue Auflage die Vorlage des unterschriebenen Formblatts *AE Form 190-16E* (nach Genehmigung) bei Antragstellung und dessen Ablage mit dem Antragspaket.

Geltungsbereich. Diese Dienstvorschrift findet Anwendung auf alle Personen, die Zugang zu kontrollierten Einrichtungen der US-Streitkräfte benötigen. Die *22d* und *80th ASG* sind berechtigt, eigene Richtlinien und Verfahren aufzustellen, die den Maßgaben dieser Dienstvorschrift entsprechen oder darüber hinaus gehen und auf ihre speziellen Bedürfnisse zugeschnitten sind.

Ergänzung. Organisationen dürfen diese Dienstvorschrift nicht ohne Genehmigung von *USAREUR PM (AEAPM-O-SO)* ergänzen.

Formulare. Diese Dienstvorschrift schreibt Formblatt *AE Form 190-16A*, *AE Form 190-16B*, *AE Form AE 190-16C*, *AE Form 190-16D* und *AE Form 190-16E* vor. Formblätter der US-Army in Europa und Formblätter höherer Dienststellen sind über das *Army in Europe Publishing System (AEPUBS)* zu beziehen.

Dokumentation. Unterlagen, die aufgrund eines in dieser Dienstvorschrift vorgeschriebenen Verfahrens erstellt wurden, sind gemäß den Vorgaben in *AR 25-400-2* zu kennzeichnen, aufzubewahren und zu vernichten. Aktenzeichen und die zur Titelaufnahme erfaßten Angaben können auf der Webseite des *Army Records Information Management System* unter <https://www.arims.army.mil> abgerufen werden.

Anmerkung: Im Zusammenhang mit der Erfassung, Bearbeitung und Weitergabe von Daten ortsansässiger Arbeitnehmer in der Bundesrepublik Deutschland (BRD) sind die Dienststellen der US-Streitkräfte verpflichtet, die Bestimmungen des *U.S. Privacy Acts* zu befolgen; ansonsten findet der *U.S. Privacy Act* als nationales US-Recht auf die ortsansässigen Arbeitnehmer in der BRD keine Anwendung.

Verbesserungsvorschläge. Die Verantwortung für diese Dienstvorschrift liegt bei *USAREUR PM (AEAPM-O-SO, DSN 381-7224)*. Verbesserungsvorschläge sind auf Formblatt *DA Form 2028* an *USAREUR PM (AEAPM-O-SO, Unit 29931, APO AE 09086-9931)*, zu richten.

Verteiler. A (*AEPUBS*).

INHALTSVERZEICHNIS

Teil I

ALLGEMEINES

1. Zweck
2. Bezugsvorschriften und -dokumente
3. Erläuterung der Abkürzungen und Begriffe
4. Allgemeines
5. Zuständigkeit
6. Richtlinien
7. Ausnahmen

Teil II

ZUGANG ZU EINRICHTUNGEN

8. Formen des Zugangs
9. Zugang mit einer *DOD ID-Card*
10. Kasernenausweise

Teil III

INSTALLATION ACCESS CONTROL SYSTEM (IACS)

11. Registrierung im *INSTALLATION ACCESS CONTROL SYSTEM (IACS)*
12. Inhaber von *DOD ID-Cards*
13. Ortsansässige Arbeitnehmer
14. Mitarbeiter verpflichteter Privatfirmen (in den USA beheimatet)
15. Mitarbeiter verpflichteter Privatfirmen (im Aufnahmeland lebend)
16. Hausangestellte
17. Zulieferer (regelmäßige Anlieferungen oder ähnliche Dienstleistungen, die nicht in Verbindung mit einem mit der US-Regierung abgeschlossenen Vertrag erbracht werden)
18. Händler und Dienstleister
19. NATO-Angehörige
20. Militärangehörige des Aufnahmestaates
21. Ausländische Lehrgangsteilnehmer (*Marshall Center*)
22. Mitglieder privater Organisationen
23. Besucher (direkte Familienangehörige, im Verantwortungsbereich von *USAREUR* lebend)
24. Besucher (Freunde, Bekannte oder Familienangehörige, die nicht unter vorstehende Personengruppe fallen)
25. Offizielle Gäste
26. Mitarbeiter des US-Außenministeriums und der US-Botschaft
27. Sonstige
28. Vertreter von Regierungsstellen/Behörden des Aufnahmestaates
29. Wachposten

Teil IV

KASERNENAUSWEIS

30. Antragsverfahren
31. Antragsverfahren für Inhaber eines befristeten Kasernenausweises
32. Antragsverfahren zur Erneuerung eines Kasernenausweises
33. Antragsverfahren bei Antrag auf Ersatz eines gestohlenen bzw. verlorengegangenen Kasernenausweises
34. Antragsverfahren zur Verlängerung eines befristeten Kasernenausweises
35. Unbrauchbare Kasernenausweise

Teil V

INSTALLATION ACCESS CONTROL OFFICE (IACO)

36. Allgemeines
37. Registrierung von Personen, die einen Kasernenausweis beantragen

38. Registrierung von Inhabern einer *DOD ID-Card*
39. Datenmäßige Erfassung von Kindern
40. Bearbeitung und Verteilung von Registrierungslisten

Teil VI

ZUGANGSFORMEN

41. Eintragung in Besucherlisten
42. Registrierungslisten
43. Einfahrt von Einsatz- und Rettungsfahrzeugen
44. *ACP*-Wachposten

Anhänge

- A. Bezugsdokumente
- B. Bestellte *Sponsoring Officials* (Musterschreiben)
- C. Formblatt AE Form 190-16A (Muster)
- D. Umrechnungstabelle für Körpergröße und Körpergewicht
- E. Anerkennung der Pflichten eines Ausweisinhabers (Musterschreiben)

Abbildungen

1. Befristeter und regulärer Kasernenausweis (Muster)
2. Formblatt *AE Form 160-19B* (Muster)
3. Erklärung zum US-Datenschutzgesetz (*U.S. Privacy Act*)

Glossar

TEIL I

ALLGEMEINES

1. ZWECK

Diese Dienstvorschrift

- a. legt Richtlinien, Aufgaben und Verfahren für den Zugang zu Einrichtungen der US-Streitkräfte in der *Area of Responsibility (AOR)* (Verantwortungsbereich) von USAREUR fest;
- b. gibt Verfahren für die Registrierung im *Installation Access Control System (IACS)* (System zur Kontrolle des Zugangs zu Einrichtungen) vor;
- c. enthält Verfahren für die Erstellung und Ausstellung von Kasernenausweisen;
- d. ist in Verbindung mit folgenden Dienstvorschriften anzuwenden:

(1) *AR 600-8-14*

(2) *AE Regulation 190-13*

(3) *AE Regulation 525-13*

(4) *USAREUR Regulation 600-700*

(5) *USAREUR Regulation 604-1*

2. BEZUGSVORSCHRIFTEN UND -DOKUMENTE

Anhang A enthält eine Liste der Bezugsdokumente.

3. ERLÄUTERUNG DER ABKÜRZUNGEN UND BEGRIFFE

Das Glossar definiert Abkürzungen und Begriffe.

4. ALLGEMEINES

a. Diese Vorschrift setzt Grundsätze für die Zugangskontrolle zu Einrichtungen fest und enthält Verfahren für die Überprüfung von Personen. Angaben zu der räumlichen Ausstattung von *Access-Control Points (ACP)* (Zugangskontrollposten) finden sich im *Technical Manual (TM)* 5-853-2 oder können vom zuständigen Beauftragten der Einrichtung für Antiterrorismus, vom Beauftragten für allgemeine Sicherheit oder von *IMA-E* zur Verfügung gestellt werden.

b. *AE Regulation 525-13* enthält Vorgaben für die Durchsuchung von Personen und Fahrzeugen.

c. Die Zugangskontrolle im *USAREUR AOR* hängt von dem effektiven Einsatz des *IACS* ab. Das *IACS*

(1) reduziert den Zugang von Personen mit gefälschten, ungültigen bzw. unzulässigen Zugangsberechtigungsdokumente zu Einrichtungen auf ein Mindestmaß;

(2) enthält eine Datenbank mit individuellen Zugangsberechtigungen;

(3) ermöglicht eine zentrale Kontrolle der Zugangsrechte (Kommandeure können beispielsweise einem gekündigten Mitarbeiter seine Zugangsberechtigung entziehen);

(4) dient der Erstellung von Kasernenausweisen;

(5) ermöglicht den Wachposten an den *ACPs* (in dieser Vorschrift als „Wachposten“ bezeichnet) mit Strichcode versehene *DOD ID-Cards* sowie Kasernenausweise zu scannen, um die Zugangsberechtigungen und Zugangsrechte zu überprüfen;

(6) dient der elektronischen Erfassung aller Personen, die Zugang zu Einrichtungen der US-Streitkräfte haben.

d. *Sponsoring Organizations* und *Sponsoring Officials* sind für den Erfolg des *Installation Access Control Program* entscheidend.

e. Welche Zugangsrechte Personen eingeräumt werden, hängt von dem Sicherheitsrisiko ab, das sie darstellen, und von der Personengruppe, der sie zuzuordnen sind (Abs. 12 bis 29).

5. ZUSTÄNDIGKEIT

a. Der *USAREUR G2*

(1) ist verantwortlich für das *Foreign National Screening Program (USAREUR-Reg 604-1)*;

(2) hat für die *FNS*-Überprüfung nicht-amerikanischer Staatsbürger ein computergestütztes System bereitzustellen;

b. Der *Inspector General* von *USAREUR* hat bei der Inspektion von Organisationen, die für Inhaber von Kasernenausweisen die Verantwortung tragen, speziell auch die korrekte Wahrnehmung der Aufgaben eines *Sponsors* zu überprüfen.

c. Der *Provost Marshal (PM)* von *USAREUR* hat

(1) die Aufsicht über das Personal und die Leitung des *Installation Access Control Program*;

(2) hat Richtlinienkompetenz und ist verantwortlich für das *IACS*. Dazu gehört, dieses bereitzustellen, zu testen, nach Ablauf seiner Lebensdauer zu ersetzen und die Anwender zu schulen;

(3) schriftliche Anträge auf Ausnahmegenehmigung von den bestehenden Richtlinien zu genehmigen;

(4) in Abstimmung mit der *Sponsoring Organization* über alle Anträge auf Ausstellung eines Kasernenausweises zu entscheiden, wenn die Personenüberprüfung zu nachteiligen Ergebnissen geführt hat und US-Streitkräfte-weiter Zugang beantragt wird;

(5) vor Ort die ordnungsgemäße Registrierung im *IACS* und die ordnungsgemäße Ausstellung von Kasernenausweisen zu überprüfen;

(6) sicherzustellen, daß alle *Installation Access Control Offices (IACOs)* die Vorgaben dieser Dienstvorschriften einhalten;

(7) die Beschaffung und sichere Verwahrung der Bestände an Blankokasernenausweisen zu überwachen;

(8) eine computergestützte Nutzungsanalyse der *IACS*-Anwender durchzuführen;

(9) in Abstimmung mit *1st Personnel Command (1st PERSCOM)* und den *Area Support Groups (ASG)* sicherzustellen, daß alle verhängten Zutrittsverbote korrekt im *IACS* erfaßt sind.

d. Der Kommandeur von *1st PERSCOM* hat

(1) sicherzustellen, daß allen Personen, denen Formblatt *AE Form 600-700A* ausgestellt wurde, bewußt ist, daß dieses kein Zugangsberechtigungsdocument darstellt und sie verpflichtet sind, sich entsprechend den Vorgaben dieser Dienstvorschrift einen Kasernenausweis ausstellen zu lassen, um Zugang zu den von den US-Streitkräften kontrollierten Einrichtungen zu erhalten;

(2) die zentrale Aufbewahrungsstelle für im gesamten Verantwortungsbereich der US-Streitkräfte geltende Zugangsverbote zur Verfügung zu stellen und Verfahren aufzustellen, um umgehend Aktualisierungen der Zugangsverbotslisten zur Verfügung zu stellen, damit das *IACS* immer den aktuellen und korrekten Stand anzeigt.

e. *ASG*-Kommandeure haben

(1) durch Aufstellen entsprechender Richtlinien sicherzustellen, daß Zugang zu den Einrichtungen der jeweiligen *Base Support Battalions (BSB)* gemäß den in dieser Dienstvorschrift vorgegebenen Richtlinien und Verfahren gewährt wird. Dabei ist zu gewährleisten, daß mit den in den verschiedenen *AGSs* und *BSBs* aufgestellten Vorgaben zur Zugangskontrolle die Bestimmungen dieser Dienstvorschrift nicht umgangen werden. *ASG*-Kommandeure dürfen z. B. keine Vorgaben aufstellen, nach denen nur von ihrem *ASG* oder einem ihrer nachgeordneten *BSBs* ausgestellte Kasernenausweise anerkannt werden. Mit dem *Installation Access Control Program* wird nämlich u.a. das Ziel verfolgt, daß die zulässigen Zugangsberechtigungsdocumente an allen Standorten der US-Streitkräfte anerkannt werden, und zwar unabhängig von ihrem Ausstellungsort. Ausgenommen sind Fälle, in denen Wachposten berechtigte Zweifel an der Authentizität eines Dokuments haben;

(2) Vorgaben zur Zugangskontrolle in das *Organization Inspection Program* aufzunehmen;

(3) Verfahren zu entwickeln, damit Entscheidungen über die Zugangsberechtigung von Personen, die einen Antrag auf Ausstellung eines Kasernenausweises stellen, deren Überprüfung aber zu nachteiligen Informationen geführt hat, mit den *Sponsoring Organizations* abgestimmt werden. Dies kann an die *BSB* übertragen werden, wenn der Zugang auf eine einzige *BSB* beschränkt ist;

(4) die Ergebnisse der Personenüberprüfung mit nachteiligen Informationen von Antragstellern, die eine Zugangsberechtigung zu mehr als einer *ASG* beantragen, an *USAREUR PM (AEAPM-O-SO), Unit 29931, APO AE 09086-9931* zu senden;

(5) durch Vorgabe entsprechender Verfahren sicherzustellen, daß der *USAREUR PM* über alle Zugangsverbote, die auf *ASG*-Ebene verhängt wurden, aber nicht im gesamten Zuständigkeitsbereich der US-Streitkräfte gelten, unterrichtet wird;

(6) in Situationen, in denen diese Vorschrift die *ASG* als *Sponsoring Organization* einsetzt, die Aufgaben der *Sponsoring Organization* zu übernehmen;

(7) den *USAREUR PM* über Zugangsmöglichkeiten zu Rate zu ziehen, wenn die durch Abs. 8a zugelassenen Zugangsmethoden nicht den gemeinsamen Nutzungsvereinbarungen mit dem Aufnahmestaat entsprechen.

f. Zusätzlich zu den in Abschnitt e oben aufgeführten Verantwortlichkeiten, haben die Kommandeure der *22d* und *80th ASG* die in diesem Kapitel vorgegebenen Richtlinien und Verfahren entsprechend abzuändern, um den speziellen Gesetzen des Aufnahmestaates gerecht zu werden (Abzuändern sind evtl. die Bestimmungen zu den erforderlichen Personenüberprüfungen, zur Abnahme von Fingerabdrücken, zur Anmeldung von Kraftfahrzeugen sowie zur Vorlage einer Aufenthalts- bzw. Arbeiterlaubnis.). Die geänderten Richtlinien und Verfahren müssen

- (1) die Sicherheitsstandards und den Zweck dieser Vorschrift wann immer möglich einhalten oder übersteigen;
- (2) mit dem *USAREUR PM* und dem *Judge Advocate (JA)* von *USAREUR* koordiniert und von ihnen genehmigt werden.

g. *BSB*-Kommandeure haben

(1) die zur Umsetzung der Vorgaben dieser Dienstvorschrift in ihrem Verantwortungsbereich erforderlichen Richtlinien und Verfahren aufzustellen. Dazu gehören u.a. folgende Anforderungen: *BSB*-Kommandeure haben

(a) durch Aufstellung entsprechender Verfahren sicherzustellen, daß alle Inhaber einer *DOD ID-Card* sich ordnungsgemäß während der Anmeldung und Abmeldung im *IACS* registrieren bzw. ihren Eintrag wieder löschen lassen. Dies kann bei dem für sie zuständigen *IACO* oder der *Central Processing Facility (CPF)* erfolgen;

(b) durch Festlegung entsprechender Verfahren sicherzustellen, daß Kasernenausweise und *DOD ID-Cards* von Personen, die keinen Zugang zu Einrichtungen mehr benötigen oder im Besitz unbrauchbarer oder abgelaufener Kasernenausweise bzw. *DOD ID-Cards* sind, eingezogen werden. Inhabern von *DOD ID-Cards* bzw. von Kasernenausweisen wird in diesem Fall Formblatt AE Form 190-16B (abrufbar unter: <https://www.aeaim.hqusareur.army.mil/library/for/index-aeef.shtm>) als Einzugs-/Empfangsbestätigung ausgestellt. Eingezogene *DOD ID-Cards* sind nicht zu vernichten. Sie sind bei der nächstgelegenen *DOD ID-Card* ausstellenden Stelle zur sachgerechten Disposition innerhalb von 24 Stunden abzugeben;

(c) für alle *IACOs* die Erstellung von Ständigen Dienstanweisungen, die der Umsetzung der in dieser Dienstvorschrift vorgegebenen Richtlinien, Verfahren und Zielsetzungen dienen, verbindlich vorzuschreiben;

(d) anzuordnen, daß für alle *Access Control Points (ACP)* (Kontrollpunkte) spezielle Anweisungen für Wachposten erstellt werden, die den Bestimmungen und Zielsetzungen dieses Kapitels in vollem Umfang gerecht werden. Diese Anweisungen haben mindestens folgende Vorgaben zu enthalten:

1. Anweisungen bzgl. der Vorgaben zur Eintragung von Personen in Besucherlisten, des Erstellens und der Gültigkeit von Registrierungslisten, der Einfahrt von Einsatz- und Rettungsfahrzeugen sowie des Vorgehens in Fällen, in denen Inhaber von *DOD ID-Cards* nicht im *IACS* registriert sind;

2. Anweisungen für die Behandlung spezieller Anträge auf Zugangsberechtigung, auf die in dieser Dienstvorschrift nicht eingegangen wird;

3. Vorgaben für die manuelle Überprüfung von Zugangsberechtigungsdocumenten bei Ausfall des *IACS*;

4. Vorgehensweise in Fällen, in denen die Fahrer die Anweisungen der Wachposten ignorieren (z. B. zur Überprüfung ihrer Zugangsberechtigung nicht anhalten);

5. Vorgaben, wie nach Erscheinen der verschiedenen Anzeigen (Eintrag archiviert, Nicht registriert) auf dem Handscanner bzw. der an den Toren bereitgestellten Computer vorzugehen ist;

6. eine Abbildung des regulären und des befristeten *USAREUR/USAFE*-Kasernenausweises sowie aller *DOD ID-Cards*;

7. eine Liste mit Telefonnummern, unter denen Mitarbeiter in Schlüsselpositionen zu erreichen sind;

8. ein Lageplan der Einrichtung;

9. Telefonnummern der wichtigsten Dienststellen auf der bewachten Einrichtung;

10. Anti-Terror-Maßnahmen und Vorgehensweise bei den verschiedenen Sicherheitsstufen;

11. Vorgaben für die Anwendung von Gewalt.

(e) der zuständigen Betriebsvertretung eine Kopie der *ACP*-Anweisungen zu übermitteln;

- (2) sicherzustellen, daß nur dazu berechnigte Nutzer Zugriff zum *IACS* haben. Die berechnigten Personen sind schriftlich zu benennen. Der Umfang ihrer Nutzungsberechnigung ist dabei anzugeben (z. B. *Registrar* oder *Super-Registrar*);
- (3) den in ihrem Verantwortungsbereich für die Einstellung von Personal zuständigen Stellen einen mit Hilfe des *IACS* erstellten Bericht zu übermitteln, in dem alle Personen aufgeführt sind, für die ein Zugangsverbot für Einrichtungen der US-Streitkräfte verhängt wurde. Dieser Bericht ist mindestens alle 3 Monate bzw. auf Anforderung zu erstellen;
- (4) sicherzustellen, daß angemessene Sicherheitsvorkehrungen für die *IACS*-Ausrüstung und -Geräte in den *IACOs*, *CPFs* und *ACPs* getroffen wurden;
- (5) sicherzustellen, dass die komplette *IACS*-Hardware, die an die *BSBs* weiter gegeben wird, für die Unterstützung von *IACS* geeignet ist;
- (6) in Situationen, in denen diese Vorschrift die *BSB* als *Sponsoring Organization* einsetzt, die Aufgaben der *Sponsoring Organization* zu übernehmen;
- (7) sicherzustellen, dass die zuständige Betriebsvertretung über die für ortsansässige Arbeitnehmer bezüglich des Zugangs/der Einfahrt in Notfällen gemäß Abs. 43 aufgestellten Verfahren informiert wird.
- h. Die *Provost Marshal Offices (PMOs)* (Militärpolizei-Dienststellen) der verschiedenen *BSBs* und *Area Support Teams (AST)* haben
- (1) nach Meldung des Verlustes oder Diebstahls einer *DOD ID-Card* bzw. eines Kasernenausweises, umgehend den Eintrag im *IACS* entsprechend zu kennzeichnen, um die gestohlene oder verlorengegangene *DOD ID-Card* bzw. den Kasernenausweis als ungültig zu kennzeichnen bzw. den Eintrag zu löschen;
- (2) zur Unterstützung der in Abs. 30b(5) für Antragsteller vorgeschriebenen Personenüberprüfung durch die Militärpolizei entsprechende Verfahren festzulegen. Kopien der Abschlussberichte sind an die *Sponsoring Organization* zu übersenden. Wenn die Überprüfungen nachteilige Ergebnisse aufweisen, sind Kopien der Abschlussberichte an die *Sponsoring Organization* und die *ASG* zu schicken. Die von der *ASG* aufgestellten Vorschriften für die Bearbeitung von Personenüberprüfungen mit nachteiligen Informationen sind einzuhalten.
- i. Alle Dienststellen, die Aufträge an Privatfirmen zur Anlieferung von Waren oder zur Durchführung von Arbeiten in kontrollierten Einrichtungen der US-Streitkräfte vergeben, haben
- (1) sicherzustellen, daß die gemäß den Vorgaben dieser Dienstvorschrift zur Ausstellung eines Kasernenausweises bzw. zur Aufnahme in eine Registrierungsliste erforderliche Personenüberprüfungen und die Vorlage einer Aufenthalts- und Arbeitserlaubnis in abgeschlossene Verträge aufgenommen werden;
- (2) in die Verträge eine Klausel aufzunehmen, in der sich die Auftragnehmer verpflichten, dafür Sorge zu tragen, daß alle ausgestellten Ausweise an das ausstellende *IACO* nach Abschluss der Arbeiten bzw. Lieferungen, oder wenn die Mitarbeiter der Firma nicht länger Zugang zu *USAREUR*-Einrichtungen brauchen (sie z. B. gekündigt haben oder entlassen wurden), abgegeben werden;
- (3) Verfahren zu entwickeln, um zu gewährleisten, dass alle beantragenden Dienststellen (k unten) in *Purchase Requests and Commitments (PR&Cs)*, *Military Interdepartmental Purchase Requests (MIPRs)* sowie in allen anderen Anträgen und Verträgen für Vertragsnehmerunterstützung folgende Informationen angeben, wenn Mitarbeiter verpflichteter Privatfirmen aufgrund des Vertrages Zugang zu Einrichtungen der US-Streitkräfte im *USAREUR AOR* benötigen:
- (a) Name der beantragenden Dienststelle sowie Name und Telefonnummer des Ansprechpartners für die Zugangskontrolle der beantragenden Dienststelle;
- (b) Ort des zuständigen *IACO* sowie Name und Telefonnummer des Ansprechpartners im *IACO*.
- j. Aufgaben des *IACO* sind in Teil V erläutert.
- k. Die *Sponsoring Organizations* haben sicherzustellen, daß
- (1) bei allen Mitarbeitern, für die sie die Verantwortung tragen, ein zwingender Grund für den Zugang zu Einrichtungen vorliegt;

(2) für alle Personen, denen ein Kasernenausweis ausgestellt werden soll, ein entsprechender Antrag (Formblatt *AE Form 190-16A*) abgefaßt wird. Der Antrag muss die Zugangserfordernisse des Antragsstellers enthalten und diese Erfordernisse wie in der Vorschrift vorgegeben begründen (z. B. wenn die Befugnis zum Eintragen von Besuchern beantragt wird);

(3) alle Personen, für die ein Antrag auf Ausstellung eines Kasernenausweises gestellt wird, überprüft werden. Wenn die Überprüfung zu nachteiligen Informationen führt, ist in Zusammenarbeit mit der *ASG*, für die die Personen tätig werden, (oder mit dem *USAREUR PM*, wenn Zugang für den gesamten Bereich der US-Streitkräfte beantragt wird,) zu entscheiden, ob diese nachteiligen Informationen eine Verweigerung der Zugangsberechtigung rechtfertigen. Wenn nachteilige Informationen zu einer Verweigerung von Zugangsrechten führen, ist der *USAREUR G2* zu benachrichtigen;

(4) die Antragsteller ihr Fahrzeug gemäß den Vorgaben dieser Dienstvorschrift und *AE-Regulation 190-1* anmelden (soweit zutreffend). Wer einen Antrag auf Aufstellung eines Kasernenausweises stellt und mit einem Privatfahrzeug in Einrichtungen der US-Streitkräfte einfahren will, hat dieses Fahrzeug anzumelden. Fahrzeuge von verpflichteten Privatfirmen gelten in Zusammenhang mit dieser Dienstvorschrift nicht als Privatfahrzeuge;

(5) folgende Informationen in *PR&Cs*, *MIPRs* sowie allen anderen Anträgen und Verträgen für Vertragsnehmerunterstützung angegeben sind, wenn Mitarbeiter verpflichteter Privatfirmen aufgrund eines solchen Vertrages Zugang zu Einrichtungen der US-Streitkräfte im *USAREUR AOR* benötigen:

(a) Name der beantragenden Dienststelle sowie Name und Telefonnummer des Ansprechpartners für die Zugangskontrolle der beantragenden Dienststelle;

(b) Ort des zuständigen *IACO* sowie Name und Telefonnummer des Ansprechpartners im *IACO*.

ANMERKUNG: Als Alternative zu (a) und (b), oben, können *Sponsoring Organizations* in Fällen, in denen es tatsächlich so ist, folgende Erklärung angeben: “*This contract will not result in a contractor requiring access to a USAREUR installation*”. (Im Rahmen dieses Vertrages benötigt kein Mitarbeiter einer verpflichteten Privatfirma Zugang zu einer Einrichtung der US-Streitkräfte.)

(6) Mitarbeiter im Bereich Vertragswesen außerhalb des *United States Army Contracting Command, Europe*, über die Vorschriften zur Zugangskontrolle in dieser Vorschrift informiert sind;

(7) bei Änderung oder Beendigung des Vertragsverhältnisses, das die Grundlage für die Ausstellung eines Kasernenausweises bildete, die Kasernenausweise eingezogen und beim zuständigen *IACO* abgegeben werden;

(8) für alle Mitarbeiter, für die sie verantwortlich sind, eine Akte mit den dazugehörigen Unterlagen angelegt wird;

(9) halbjährlich mit dem zuständigen *IACO* eine Überprüfung vorgenommen wird, um zu gewährleisten, daß alle Personen, für die sie verantwortlich sind, korrekt in der *IACS*-Datenbank erfaßt sind;

(10) dem zuständigen *IACO* in einem entsprechenden Schreiben die Namen der Personen mitgeteilt werden, die im Auftrag ihrer *Sponsoring Organization* (Anhang B) Aufgaben in Zusammenhang mit der Ausweisausstellung (*Sponsoring Officials*) wahrnehmen;

(11) die in Abs. 30c vorgegebenen Verfahren eingehalten werden, wenn der *Sponsoring Official* den Antragsteller nicht zum zuständigen *IACO* begleiten kann.

1. Personen, die wiederholt und ohne Begleitung Zugang zu Einrichtungen der US-Streitkräfte benötigen und denen Zugang unter Vorlage einer *DOD ID-Card* bzw. eines Kasernenausweises zu gewähren ist, haben

(1) der Abnahme von digitalisierten Fingerabdrücken unter nachstehenden Voraussetzungen zuzustimmen:

(a) Anmeldung: Wer bereits im Besitz einer zulässigen, maschinell erstellten *DOD ID-Card* ist, hat sich während der Anmeldung beim zuständigen *IACO* bzw. *CPF* digitalisierte Fingerabdrücke abnehmen zu lassen. Inhaber manuell erstellter *DOD ID-Cards* haben sich eine maschinell erstellte, mit Strichcode versehene *DOD ID-Card* ausstellen zu lassen, unter Einhaltung der in einschlägigen Militärdienstvorschriften und Personalverwaltungssystemen vorgeschriebenen Verfahren.

(b) Beantragung eines Kasernenausweises: Personen, die nicht im Besitz einer zugelassenen *DOD ID-Card* sind und wiederholt und ohne Begleitung Zugang zu Einrichtungen der US-Streitkräfte im *USAREUR AOR* benötigen, haben einen Kasernenausweis zu beantragen. Die Ausstellung des Kasernenausweises erfolgt erst nach Vorlage der dafür erforderlichen Dokumente beim zuständigen *IACO* und nach Abnahme digitalisierter Fingerabdrücke.

(2) ihre *DOD ID-Card* bzw. ihren Kasernenausweis im Dienst und bei Aufenthalt in einer Einrichtung der US-Streitkräfte stets bei sich zu tragen. Auf Aufforderung sind die *DOD ID-Card* bzw. der Kasernenausweis der Militärpolizei und Wachposten vorzuzeigen. Kommt ein Antragsteller einer solchen Aufforderung nicht nach, kann dies zum unverzüglichen Einzug des Ausweises führen und verwaltungsrechtliche oder Strafmaßnahmen nach sich ziehen;

(3) den Verlust bzw. den Diebstahl ihrer *DOD ID-Card* bzw. ihres Kasernenausweises umgehend der örtlichen Militärpolizei oder dem zuständigen *IACO* zu melden, damit der Ausweis sofort als ungültig gekennzeichnet werden kann;

(4) die *Sponsoring Organization* über jede Änderung des dienstlichen Verhältnisses, das die Grundlage für die Zugangsberechtigung bildet, zu informieren;

(5) den Kasernenausweis beim zuständigen *IACO* bzw. bei der *Sponsoring Organization* abzugeben, wenn dieser abgelaufen ist oder wenn die Voraussetzung für den Besitz des Ausweises nicht länger gegeben ist;

(6) bei beabsichtigter Einfahrt in Einrichtungen der US-Streitkräfte mit einem Privatfahrzeug, dieses Fahrzeug im Rahmen der Beantragung eines Kasernenausweises anzumelden. Fahrzeuge von verpflichteten Privatfirmen gelten in Zusammenhang mit dieser Vorschrift nicht als Privatfahrzeuge.

m. Absatz 44 schreibt die Aufgaben der *ACP*-Wachposten vor.

6. RICHTLINIEN

a. Aufgabe der Kommandeure ist es, die Sicherheit ihrer Einrichtungen zu gewährleisten und die Umsetzung und Einhaltung der Bestimmungen dieser Dienstvorschrift sicherzustellen. Sollte die Einhaltung mit Schwierigkeiten verbunden sein, ist dies kein Grund, die in dieser Dienstvorschrift vorgeschriebenen Verfahren zu umgehen oder zu modifizieren. Die vorgeschriebenen Verfahren tragen bei zur

(1) besseren Einhaltung der bzgl. der Zugangskontrolle getroffenen Sicherheitsmaßnahmen;

(2) eindeutigen Identifizierung von Personen, denen kein Zugang zu gewähren ist, an den *ACPs* zu Einrichtungen der US-Streitkräfte;

(3) Verhütung einer unrechtmäßigen Aneignung und des Diebstahls von Regierungseigentum sowie des unrechtmäßigen Einschleusens von Waffen, Sprengstoffen und anderer verbotener Waren in Einrichtungen der US-Streitkräfte.

b. Abnahme von Fingerabdrücken:

(1) Anmeldung: Alle Personen, die im Besitz einer zugelassenen *DOD ID-Card* sind, sowie alle Personen, die einen Antrag auf Ausstellung eines Kasernenausweises stellen, haben sich bei der Registrierung im *IACS* digitalisierte Fingerabdrücke abnehmen zu lassen.

(2) Überprüfung der Identität: Sicherheitsbeamte bzw. für die Sicherheit zuständige Angehörige des Kommandos können zur Überprüfung der Identität von Personen diese auffordern, sich digitalisierte Fingerabdrücke abnehmen zu lassen. Diese Form der Überprüfung kann routinemäßig an den *ACPs* von Einrichtungen der US-Streitkräfte erfolgen. Sie kann allerdings nicht nur an den an den Toren bzw. Zufahrten eingerichteten *ACPs* erfolgen, sondern auch jenseits dieser *ACPs*. Eine Verweigerung der Abnahme digitalisierter Fingerabdrücke kann den unmittelbaren Einzug des Kasernenausweises bzw. der *DOD ID-Card* zur Folge haben und zu verwaltungsrechtlichen oder arbeitsrechtlichen Maßnahmen durch das Kommando führen.

(a) Wird ein Bürger des Aufnahmestaates festgehalten oder durchsucht, hat dies in Abstimmung mit der Polizei des Aufnahmestaates zu erfolgen. Handelt es sich um einen ortsansässigen Arbeitnehmer, ist während der regulären Arbeitszeit zusätzlich die zuständige Betriebsvertretung hinzuzuziehen. Wird ein ortsansässiger Arbeitnehmer außerhalb der regulären Arbeitszeit festgehalten oder durchsucht, ist die zuständige Betriebsvertretung unverzüglich am nächsten Arbeitstag zu unterrichten.

(b) Die für den Zugang zu Einrichtungen aufgestellten Richtlinien basieren auf einer Überprüfung der Zugangsberechtigung aller Personen, die eine kontrollierte Einrichtung der US-Streitkräfte betreten; sie basieren nicht auf einer Überprüfung der Fahrzeuge oder anderer Transportmittel, mit denen in die Einrichtungen eingefahren wird. Deshalb ist die Zugangsberechtigung aller Insassen eines Fahrzeugs oder eines anderen Transportmittels gemäß den in dieser Dienstvorschrift aufgestellten Richtlinien und Verfahren zu überprüfen.

(3) Über eine Personenauthentifizierung hinausgehende Überprüfung der Identität: Geht die Aufforderung zur Abnahme digitalisierter Fingerabdrücke über die Feststellung der Identität einer Person hinaus, hat für jedes Festhalten oder jede Durchsuchung ein „triftiger Grund“ bzw. eine rechtliche Grundlage vorzuliegen. Eine Koordinierung mit dem zuständigen *Judge Advocate Office* (wenn zweckmäßig) hat zu erfolgen, wenn die Aufforderung zur Abnahme von Fingerabdrücken zu einem Festhalten oder einer Durchsuchung führt.

ANMERKUNG: Die Vorgaben in vorstehendem Abs. (3) gelten nur für US-Bürger.

7. AUSNAHMEN

a. Personen, die einen Antrag auf Ausnahmegenehmigung von in dieser Dienstvorschrift aufgestellten Bestimmungen stellen, müssen ihre Anträge auf dem vorgeschriebenen Dienstweg an *USAREUR PM (AEAPM-O-SO), Unit 29931, APO AE 09086-9931* oder per E-Mail an *iacs@manupo.pmo.army.mil* senden.

b. Ausnahmegenehmigungen, die nach Inkrafttreten dieser Dienstvorschrift erteilt werden, können für die Dauer von bis zu 1 Jahr vom *USAREUR PM* bewilligt und genehmigt werden. Eine längere Gültigkeitsdauer ist nur zulässig, wenn diese vom *USAREUR PM* ausdrücklich schriftlich genehmigt wird.

c. Ausnahmegenehmigungen, die im Rahmen der *IACS*-Softwareanwendungen eingebaut sind, können örtlich geregelt werden und erfordern keine Genehmigung vom *USAREUR PM*.

d. Ausnahmegenehmigungen von Bestimmungen in Abschnitt 8b unterliegen diesem Abschnitt nicht.

Teil II

ZUGANG ZU EINRICHTUNGEN

8. FORMEN DES ZUGANGS

a. Zugang zu Einrichtungen der US-Streitkräfte im *USAREUR AOR* wird hauptsächlich unter vier Voraussetzungen gewährt. Zugangsberechtigt sind Personen, die

(1) im Besitz einer gültigen *DOD ID-Card* und im *IACS* erfasst sind (Ausnahmen von der vorgeschriebenen Erfassung im *IACS*, s. Abs. 44e);

(2) im Besitz eines regulären oder eines befristeten *USAREUR/USAFE*-Kasernenausweises sind;

ANMERKUNG: Ausweisinhabern, die aus dienstlichen bzw. operativen Gründen vorübergehend Zugang zu weiteren Einrichtungen als den auf ihrem Ausweis aufgeführten benötigen, kann bei Vorlage eines gültigen Kasernenausweises zusammen mit einer Dienstreiseanordnung Zugang gewährt werden. Personen mit einem gültigen Besucherausweis, die vorübergehend Zugang zu weiteren Einrichtungen als den auf ihrem Ausweis aufgeführten benötigen, wird in Begleitung der beantragenden Person dieser erweiterte Zugang ebenfalls gewährt. Im Folgenden sind beispielhaft Fälle aufgeführt, in denen erweiterter Zugang vorübergehend gewährt werden kann:

Beispiel 1: Kasernenausweisinhaber, denen lediglich eine für das *6th ASG* gültige Zugangsberechtigung ausgestellt wurde, die aber zu Schulungszwecken Zugang zu Einrichtungen des *26th ASG* benötigen, können z. B. bei Vorlage ihres Kasernenausweises zusammen mit der entsprechenden Dienstreiseanordnung Zugang zu diesen Einrichtungen erhalten. Aus der Dienstreiseanordnung haben Ort, Datum und Zeiten der Schulung hervorzugehen. Da nicht in all diesen Situationen Dienstreiseanordnungen ausgestellt werden, sind auch andere Unterlagen, aus denen der Zweck sowie der Ort und das Datum der Schulung hervorgehen, zugelassen.

Beispiel 2: Personen, denen ein Besucherausweis für das *293. BSB* ausgestellt wurde und welche die den Zugang beantragende Person während ihres Besuchs ins *415. BSB* begleiten, kann Zugang zu diesem *BSB* gewährt werden, ohne dass sie in eine Besucherliste eingetragen werden müssen.

(3) von einer dazu berechtigten Person in eine Besucherliste eingetragen sind;

(4) auf einer genehmigten Registrierungsliste verzeichnet sind und eines der in Abs. 30d(1) aufgeführten Dokumente vorlegen.

b. Wenn möglich, wird Zugang unter den in vorstehendem Abs. a beschriebenen Voraussetzungen gewährt. Dabei sind die in dieser Dienstvorschrift enthaltenen Bestimmungen und Verfahren einzuhalten. In bestimmten Fällen haben Kommandeure möglicherweise die Voraussetzungen aus operativen Gründen zu ergänzen (z. B. bei großangelegten Übungen, an denen Angehörige ausländischer Streitkräfte teilnehmen, für Laufformationen beim Frühsport oder für die Einfahrt von Militärkonvois). Ausnahmen von den Bestimmungen in vorstehendem Abs. a sind in *BSB-Richtlinien* zu erläutern und vom ASG-Kommandeur zu genehmigen. Die Bestimmungen in diesem Abschnitt negieren die Bestimmungen in Abs. 7 nicht.

c. Vorgaben für die Einfahrt von Einsatz- und Rettungsfahrzeugen, s. Abs. 43.

d. Aufgrund von dienstlichen Mitteilungen, Dienstreiseanordnungen/Abkommandierungen, Formblatt *AE Form 600-700A*, US-Pässen, von den Entsendestaaten der NATO (Belgien, Frankreich, Großbritannien, Kanada und den Niederlanden) ausgestellten Ausweisen sowie Formblatt *DD Form 1172* ist kein Zugang zu gewähren. Personen, die im Besitz dieser Dokumente sind, sind von einer hierzu berechtigten Person in eine Besucherliste einzutragen. Alle Personen, denen aufgrund eines dieser oder anderer Dokumente wiederholt und ohne Begleitung Zugang gewährt wurde, müssen sich unter Angabe der entsprechenden Personenkategorie (Abs. 12 bis 29) einen Kasernenausweis ausstellen lassen.

e. Standortkommandeure sind nicht berechtigt, weitere Beschränkungen zu verfügen, es sei denn es besteht dazu eine begründete Notwendigkeit (z. B. wenn die Einrichtung über schutzwürdige Mittel oder Sicherheitsbereiche verfügt und keine auf verschiedenen Ebenen greifenden Sicherheitsmaßnahmen vorhanden sind). In solchen Fällen können Kommandeure bestimmen, daß zusätzliche Dokumente (wie z. B. ein Sonderausweis) vorgelegt werden, um Zugang zu ihren Einrichtungen zu erhalten. Kommandeure sind allerdings nicht berechtigt, Zugang lediglich aufgrund dieser Dokumente zu gewähren und auf die Vorlage einer *DOD ID-Card* bzw. eines *USAREUR/USAFE-Kasernenausweises* (regulär und befristet) zu verzichten.

f. Obwohl ein US-Paß kein gültiges Zugangsberechtigungsdocument darstellt, haben die Wachen in Notfällen (z. B. beim Wechsel zu Sicherheitsstufe Delta) US-Bürgern, die nicht im Besitz einer *DOD ID-Card* oder eines Kasernenausweises sind, den Zugang nicht zu verwehren. In solchen Situationen haben sich die Wachen zur Unterstützung umgehend mit der Militärpolizei in Verbindung zu setzen. Die Militärpolizei trifft den US-Bürger am *ACP* und wird angemessene Unterstützung leisten.

9. ZUGANG MIT EINER *DOD ID-CARD*

a. Der Besitz einer *DOD ID-Card* berechtigt ihre Inhaber nicht automatisch zum Zugang zu Einrichtungen der US-Streitkräfte im *USAREUR AOR*. Die *DOD ID-Card* hat einen lesbaren Strichcode aufzuweisen und ihr Inhaber muß im *IACS* erfaßt sein, soweit nicht die in Abs. 44e aufgeführte Ausnahmeregelung für die vorgeschriebene Erfassung Anwendung findet. Personen, die im Besitz einer manuell erstellten *DOD ID-Card* sind, haben sich gemäß den Vorgaben in einschlägigen Militärdienstvorschriften und Personalverwaltungssystemen eine maschinell erstellte, mit Strichcode versehene *DOD ID-Card* ausstellen zu lassen.

b. Die folgenden maschinell erstellten *DOD ID-Cards* (*AR 600-8-14*) gelten als gültige Zugangsberechtigungsdocumente:

(1) *DD Form 2* (ACT). Diese grüne Karte wird an Angehörige des aktiven Dienstes ausgegeben. Sie wird durch die *Common Access Card* (CAC) ((9) unten) ersetzt.

(2) *DD Form 2*, (RET). Diese blaue Karte wird an Militärangehörige ausgegeben, die aus dem aktiven Dienst ausgeschieden sind.

(3) *DD Form 2*, (RES). Diese grüne Karte wird an Angehörige der Reserve oder der Nationalgarde ausgegeben. Sie wird durch die *CAC* ersetzt.

(4) *DD Form 2*, (RES RET). Diese rote Karte wird an Angehörige der Reserve und der Nationalgarde ausgegeben, die aus dem Dienst ausgeschieden sind.

(5) *DD Form 1173*. Diese braune Karte wird an berechtigte Familienangehörige der Militär- und Zivilbediensteten des US-Verteidigungsministeriums ausgegeben.

(6) *DD Form 1173-1*. Diese rote Karte wird an berechtigte Familienangehörige der Reserve und der Nationalgarde und von Zivilbediensteten des US-Verteidigungsministeriums ausgegeben.

(7) *DD Form 1934*. Diese Karte wird an Angehörige des Sanitätsdienstes und der Militärseelsorge sowie des medizinischen Hilfspersonals, die bei in Krisengebiete verlegten US-Streitkräften dienen oder diese dorthin begleiten, und die durch den Feind in Kriegsgefangenschaft geraten könnten.

(8) *DD Form 2765*. Diese braune Karte wird an Träger der „*Medal of Honor*“ ausgegeben sowie an Veteranen, die aufgrund einer mit ihrem Wehrdienst in Zusammenhang stehenden Verletzung oder Krankheit von der *Veteran's Administration* als 200% dienstuntauglich eingestuft und ehrenhaft aus der Armee entlassen wurden (ausgenommen sind aktive Militäranghörige oder aus dem aktiven Dienst ausgeschiedene Militäranghörige).

(9) *CAC*

c. Folgendes findet auf US-Zivilbedienstete, denen aufgrund der vom US-Verteidigungsministerium verhängten Ausstellungssperre keine *CAC* ausgestellt werden kann, Anwendung:

(1) Definition: Aufgrund der vom US-Verteidigungsministerium verhängten Ausstellungssperre für *CAC-Cards* an bestimmte US-Zivilbedienstete haben die *IACOs* den betroffenen Zivilbediensteten bei entsprechender Berechtigung nach ihrer Einstellung befristete Kasernenausweise auszustellen, wenn diesen keine *CAC-Card* ausgestellt werden kann, sie aber dennoch Zugang zu *USAREUR/USAFE* Einrichtungen benötigen.

ANMERKUNG: Dies betrifft nur neu eingestellte zivile US-Mitarbeiter (die neu bei den US-Streitkräften beschäftigt sind) sowie US-Zivilbedienstete, die von einer Organisation des US-Verteidigungsministeriums in eine andere wechseln (z. B. von der Luftwaffe zu den Landstreitkräften). Auf Zivilbedienstete, die bereits bei den US-Streitkräften beschäftigt sind und innerhalb einer Teilstreitkraft versetzt oder umgesetzt werden, findet diese Regelung keine Anwendung.

(2) Folgende Ausweise können ausgestellt werden:

(a) Befristeter Kasernenausweis: Er kann Personen, die dieser Gruppe angehören, ausgestellt werden.

(b) Kasernenausweis: Er darf diesen Personen nicht ausgestellt werden.

(3) Gültigkeitsdauer des Ausweises: Befristete Kasernenausweise sind maximal 90 Tage gültig.

(4) Erfordernisse bzgl. eines Sponsors: Das *Civilian Personnel Advisory Center (CPAC)* hat für diese Personen die in dieser Dienstvorschrift beschriebenen Aufgaben eines *Sponsors* wahrzunehmen.

(5) Personenüberprüfungen: Sind für diese Personengruppe nicht erforderlich.

(6) Aufenthalts- und Arbeitserlaubnis: Die Vorlage dieser Dokumente ist nicht erforderlich.

(7) Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen der Ausweisinhaber Zugang erhält: Beschränkungen bestehen keine. Außerhalb den USA eingestellten zivilen Mitarbeitern wird automatisch Zugang zu Einrichtungen der US-Streitkräfte gewährt. Eine Begründung ist hierfür nicht erforderlich.

(8) Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Personen dieser Gruppe Zugang gewährt wird, bestehen keine.

(9) Beschränkungen bzgl. der Berechtigung, Personen in Besucherlisten einzutragen: Personen dieser Personengruppe dürfen höchstens 4 Personen mit ihren Fahrzeugen eintragen.

(10) Sicherheitsstufenbezogene Beschränkungen: In Zusammenhang mit den Sicherheitsstufen bestehen keine Zugangsbeschränkungen.

ANMERKUNG: Alle CACs bestehen aus weißen Plastikkarten ohne kennzeichnende Farbmarkierungen. CACs mit einem grünen Streifen werden an Personen ausgegeben, die die US-Staatsbürgerschaft besitzen und im Rahmen eines mit dem US-Verteidigungsministerium geschlossenen Vertrages bei den US-Streitkräften tätig werden. Für den Zweck der Registrierung im IACS sind diese Personen als Inhaber einer DOD ID Card zu betrachten und ist ihr Antrag entsprechend zu bearbeiten. Auf der Rückseite von CAC-Cards, die keinen Zugang zu militärischen Einrichtungen gewähren (wie sie in der Regel an Familienangehörige, die außerhalb den USA eingestellt werden, oder in den USA an Zivilbedienstete oder Mitarbeiter verpflichteter Privatfirmen ausgestellt werden), ist keine Social Security Number (Sozialversicherungsnummer) angegeben. Ihre Inhaber sind dennoch zum Zwecke der Registrierung im IACS wie DOD ID-Card Inhaber zu erfassen. CACs mit einem roten Längsstreifen auf der rechten Seite werden nicht als gültige Zugangsberechtigungsdokumente anerkannt. Die mit einem roten Längsstreifen gekennzeichneten CACs werden ortsansässigen Arbeitnehmern ausgestellt, die sich zum Zugang zu Einrichtungen gemäß Abs. 13 Kasernenausweise ausstellen lassen müssen.

10. KASERNAUSWEISE

a. USAREUR stellt zwei Arten von Kasernenausweisen aus: den USAREUR/USAFE Installation Pass und den Temporary USAREUR/USAFE Installation Pass, in dieser Dienstvorschrift als (regulärer) Kasernenausweis bzw. befristeter Kasernenausweis bezeichnet.

b. Zur Unterscheidung der beiden Ausweise weist das für die Bezeichnung vorgesehene Feld beim befristeten Kasernenausweis einen roten Hintergrund auf, das beim regulären Kasernenausweis einen grünen. Beide Ausweise sind in Abb. 1 abgebildet. Die beiden Ausweise weisen zwar ein ähnliches Aussehen auf, die mit dem jeweiligen Ausweis verbundenen Einschränkungen eines jeden Ausweises sind allerdings verschieden.

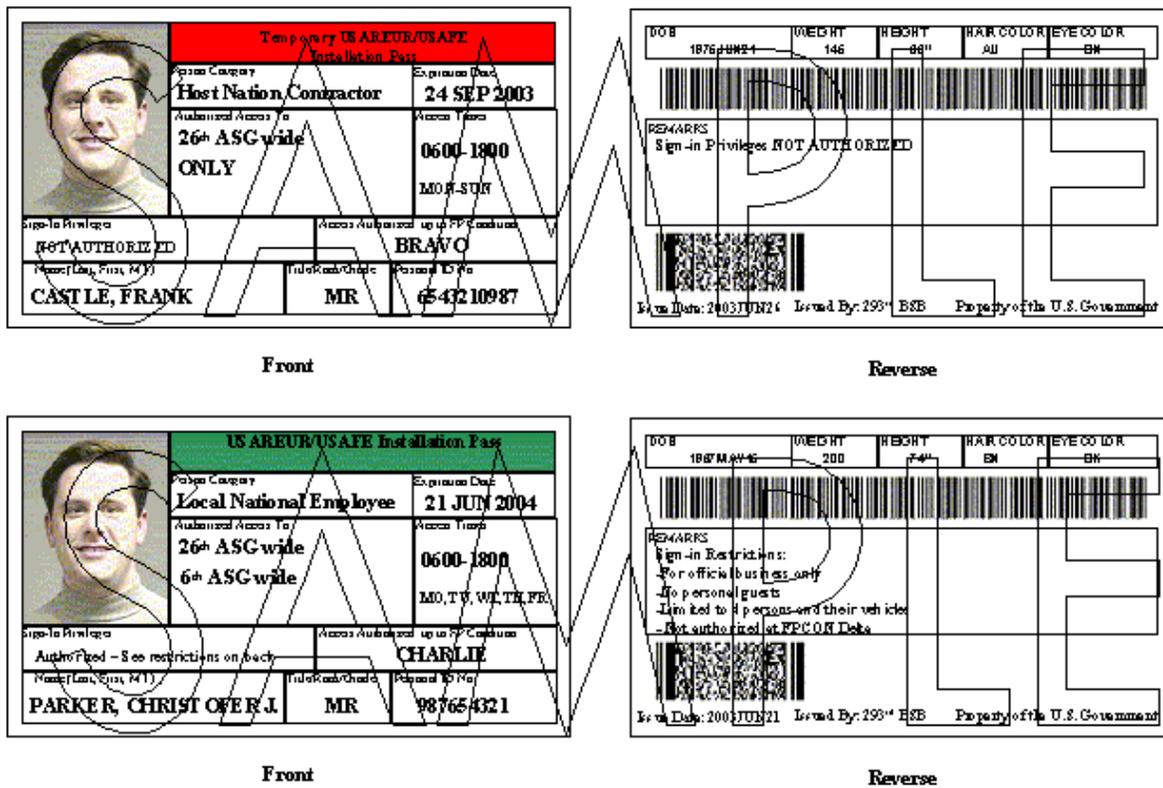


Abbildung 1: Muster Befristeter USAREUR/USAFE-Kasernenausweis und USAREUR/USAFE-Kasernenausweis

c. Die IACOs sind nicht berechtigt, das Aussehen der Ausweise durch Anbringen ASG- bzw. BSB-spezifischer Kennzeichen zu verändern (z.B. eigene Stempel, Aufkleber oder Hologramme).

d. Die beiden Kasernenausweise unterscheiden sich u.a. in Folgendem:

(1) Die Gültigkeitsdauer befristeter Kasernenausweise ist auf 90 Tage begrenzt.

(2) Soll ein regulärer Kasernenausweis ausgestellt werden, kann bis zum Abschluss der erforderlichen Personenüberprüfungen ein befristeter Kasernenausweis ausgestellt werden. Damit wird Sicherheitsbedenken und operativen Erfordernissen gleichermaßen Rechnung getragen. Die sukzessive Ausstellung und Verwendung befristeter Kasernenausweise ist unzulässig, soweit nicht die Ausnahmeregelung in Abs. 34 Anwendung findet.

e. Die Erfordernisse für die Registrierung von Personen, die einen Kasernenausweis beantragen, im *IACS* sind in Abs. 11 aufgeführt. Die Registrierung im *IACS* kann erst nach Abschluss des Antragsverfahrens in den Abs. 12 - 29 erfolgen.

TEIL III **INSTALLATION ACCESS CONTROL SYSTEM**

11. REGISTRIERUNG IM INSTALLATION ACCESS CONTROL SYSTEM (IACS)

a. Alle Inhaber von *DOD ID-Cards*, die im Verantwortungsbereich von *USAREUR*-Dienststellen unterstellt sind, sowie alle Personen, die die Ausstellung eines Kasernenausweises beantragen, müssen im *IACS* erfasst werden. Inhaber von *DOD ID-Cards*, die auf Dienstreise oder zu Besuch im *USAREUR AOR* sind, können ebenfalls erfasst werden. Maßgebend für die Registrierung im *IACS* ist die Dauer ihres Aufenthalts. Bei zweitägigen Dienstreisen z. B. ist eine Registrierung im *IACS* nicht unbedingt erforderlich; dagegen sollten Personen, die sich auf einer einmonatigen Dienstreise/Abkommandierung befinden, im *IACS* erfasst werden.

b. Jeder Zugang eines nicht registrierten *DOD ID-Card*-Inhabers macht einen Eintrag im *IACS* erforderlich. Diese Vorgehensweise führt für nicht registrierte *DOD ID-Card*-Inhaber zu einer geringfügigen Verzögerung, wenn sie Zugang zu einer Einrichtung ersuchen. Diese Maßnahme ermöglicht aber auch, Personen zu kontrollieren, die sich als nicht-registrierte *DOD ID-Card*-Inhaber auffallend häufig Zugang zu Einrichtungen verschaffen, da dies ein Hinweis auf unrechtmäßigen Besitz einer *DOD ID-Card* sein könnte (Abs. 44e).

c. Teil IV enthält die Verfahren für die Beantragung von Kasernenausweisen.

d. Eine Person kann für eine der folgenden Personenkategorien in Frage kommen:

(1) Inhaber von *DOD ID-Cards*

(2) Ortsansässige Arbeitnehmer

(3) Mitarbeiter verpflichteter Privatfirmen (in den USA beheimatet)

(4) Mitarbeiter verpflichteter Privatfirmen (im Aufnahmeland lebend)

(5) Hausangestellte

(6) Zulieferer (regelmäßige Anlieferungen oder ähnliche Dienstleistungen, die nicht in Verbindung mit einem mit der Regierung abgeschlossenen Vertrag erbracht werden)

(7) Händler, Dienstleister

(8) NATO-Angehörige

(9) Militärangehöriger des Aufnahmestaates

(10) Ausländische Lehrgangsteilnehmer (Marshall Center)

(11) Mitglieder privater Organisationen

(12) Besucher (direkte Familienangehörige, in Europa lebend)

(13) Besucher (Bekannte, Freunde oder Familienangehörige, die nicht in vorstehende Gruppe fallen)

- (14) Offizielle Gäste
- (15) Mitarbeiter des US-Außenministeriums und der US-Botschaft
- (16) Sonstige
- (17) Vertreter von Regierungsstellen/Behörden des Aufnahmestaates
- (18) Wachposten

e. Personen, die zwei verschiedenen Personengruppen zugerechnet werden könnten (z. B. ein aus dem aktiven Dienst ausgeschiedener Militärangehöriger, der für eine verpflichtete Privatfirma tätig ist), sind unter der Gruppe zu erfassen, die ihnen die größten Zugangsrechte gewährt. Die Gruppen "Offizielle Gäste" (d(14) oben) und "Sonstige" (d(16) oben) sind für Personen, die zwei Personengruppen zugerechnet werden könnten, nicht als eine der Kategorien heranzuziehen.

f. Die Zuordnung zu den verschiedenen Personengruppen in d oben hängt vom Sicherheitsrisiko ab, das die Personen evt. darstellen könnten. Welche Voraussetzungen für eine Registrierung im *IACS* erfüllt sein müssen und welche Zugangsbeschränkungen zu verfügen sind, ist in Abs. 12 bis 29 erläutert.

12. INHABER VON *DOD ID-CARDS*

a. Definition: Hierunter fallen alle Personen, denen eine *DOD ID-Card* ausgestellt werden kann, einschließlich Kinder und Jugendliche unter 18 Jahren. Der Status als *DOD ID-Card*-Inhaber hat Vorrang vor allen anderen Personengruppen (Abs. 11d(2) bis (18)). Ortsansässige Arbeitnehmer, die mit US-Militärangehörigen verheiratet sind und deshalb Anspruch auf Formblatt *DD Form 1173* haben, sind z. B. in diesem Zusammenhang als Inhaber einer *DOD ID-Card* zu behandeln. Ihnen wird kein Kasernenausweis ausgestellt. Außerdem ist keine Organisation bzw. Person zu bestimmen, die für sie die Aufgaben eines *Sponsors* übernimmt.

b. Folgende Ausweise können ausgestellt werden: Inhaber von *DOD ID-Cards* erhalten ihre *ID-Card* unter Anwendung der in einschlägigen Militärdienstvorschriften und Personalverwaltungssystemen aufgestellten Verfahren. Die Inhaber dieser Ausweise sind in dem für sie zuständigen *IACO* bzw. der zuständigen *CPF* bei der Anmeldung datentechnisch zu erfassen und dann im *IACS* zu registrieren. Ihnen wird kein Kasernenausweis ausgestellt. Inhaber einer manuell erstellten *DOD ID-Card* haben sich eine maschinell erstellte (mit Strichcode versehene) *DOD ID-Card* ausstellen zu lassen. Personen, die im Besitz mehrerer *DOD ID-Cards* sind (z.B. aus dem aktiven Dienst ausgeschiedene Militärangehörige, die nun als Zivilbedienstete des US-Verteidigungsministeriums, Abt. Heer tätig sind) müssen sich entscheiden, welche *DOD ID-Card* sie für die Registrierung im *IACS* nutzen wollen und müssen diese Karte beim Zugang zu Einrichtungen vorzeigen.

c. Gültigkeitsdauer der Registrierung: Die Registrierung ist bis zum Ablauf der *DOD ID-Card* gültig. Die Gültigkeitsdauer der Registrierung hat 5 Jahre nicht zu überschreiten. Bei Personen, die sich nur vorübergehend im *USAREUR AOR* (z.B. auf Dienstreise) aufhalten, ist für die Gültigkeitsdauer der Registrierung das Ende ihres Aufenthalts maßgebend.

ANMERKUNG: Da im *IACS* immer ein Datum bestimmt wird, zu dem die Registrierung ihre Gültigkeit verliert, haben Personen, deren Dienstzeit verlängert wird (z. B. Soldaten mit einer genehmigten Verlängerung ihrer Dienstzeit im Ausland) das für sie zuständige *IACO* bzw. *CPF* aufzusuchen, um die Gültigkeitsdauer im *IACS* zu aktualisieren.

d. Erfordernisse bzgl. eines Sponsors: Im Gegensatz zu Personen in anderen Gruppen, können Inhaber von *DOD ID Cards* als ihr eigener Sponsor fungieren und müssen auch keinen Antrag auf Ausstellung eines Ausweises (*AE Form 190-16A*) stellen. Inhaber einer *DOD ID-Card* haben dem für sie zuständigen *IACO* bzw. *CPF* alle für die Registrierung im *IACS* erforderlichen Unterlagen vorzulegen. In vielen Fällen ist die Gültigkeitsdauer der vorgelegten Dokumente maßgebend für die Gültigkeitsdauer der Registrierung. Die Vorlage folgender Unterlagen ist zulässig, ist allerdings nicht auf diese beschränkt: Versetzungs- und Dienstreiseanordnungen bzw. Abkommandierungen, Formblatt *DA Form 31*, *SF 50-B* oder *DA Form 3434*. Mit der geforderten Vorlage dieser Dokumente soll verhindert werden, daß Personen, die illegal im Besitz einer *DOD ID-Card* sind, im *IACS* erfaßt werden. Minderjährige sind bei der Registrierung von einem Elternteil oder einem Vormund zu begleiten.

e. Personenüberprüfungen: Personenüberprüfungen entfallen für Inhaber von *DOD ID-Cards*.

f. Aufenthalts- und Arbeitserlaubnis: Inhaber von *DOD ID-Cards* benötigen keine Aufenthalts- oder Arbeitserlaubnisse.

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen Inhaber von DOD ID-Cards Zugang gewährt wird: Keine, es sei denn ein dazu befugter Kommandeur verfügt solche Beschränkungen.

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Keine, es sei denn ein dazu befugter Kommandeur verfügt solche Beschränkungen.

i. Beschränkung der Berechtigung, Personen in Besucherlisten einzutragen: Diese Berechtigung wird erst ab einem Alter von 18 Jahren gewährt (Ausnahme: Angehörige des aktiven Dienstes) und ist auf vier Personen mit Fahrzeugen begrenzt. Ansonsten gelten keine Beschränkungen, es sei denn ein dazu befugter Kommandeur verfügt Beschränkungen.

ANMERKUNG: Je nach Sachlage können Kommandeure nach Rücksprache mit dem zuständigen *Staff Judge Advocat* (militärischer Rechtsberater) und dem *IACO* Zugangsberechtigungen bzw. -rechte beschränken oder auch entziehen.

j. Sicherheitsstufenbezogene Beschränkungen: Keine

13. ORTSANSÄSSIGE ARBEITNEHMER

a. Definition: Hierunter fallen alle Personen, die im Dienst des US-Verteidigungsministeriums im *USAREUR AOR* tätig sind, aber keinen Anspruch auf eine in Abs. 9 aufgeführte *DOD ID-Card* haben. Dieser Gruppe gehören hauptsächlich ortsansässige Arbeitnehmer im *USAREUR AOR* an.

ANMERKUNG: Da laut Vorgaben des US-Verteidigungsministeriums in absehbarer Zukunft alle Computernutzer für die Anmeldung in einem von der Regierung bereitgestellten Computer im Besitz einer *CAC* sein müssen, kann ortsansässigen Arbeitnehmern eine solche Karte ausgestellt werden. Die ortsansässigen Arbeitnehmern ausgestellten *CACs* weisen auf der rechten Seite einen roten Längsstreifen auf. Diese *CACs* sind nicht als Zugangsberechtigungsdokumente zu Einrichtungen zu verwenden.

b. Folgende Ausweise können ausgestellt werden:

(1) Befristeter Kasernenausweis: Befristete Kasernenausweise werden erst ausgestellt, nachdem alle erforderlichen Personenüberprüfungen abgeschlossen sind und eine *FNS*-Überprüfung in die Wege geleitet wurde. Befristete Kasernenausweise sind lediglich bis zur Ausstellung regulärer Kasernenausweise zu verwenden.

(2) Kasernenausweis: Kann nach Abschluss aller Personenüberprüfungen (einschl. der *FNS*-Überprüfung) mit negativem Ergebnis (ohne Eintragungen) ausgestellt werden.

ANMERKUNG: Personenüberprüfungen, die ergeben, dass Eintragungen vorliegen, sind an die *ASG*, in der der Antragsteller tätig wird, zur Entscheidung weiterzuleiten. Die Kommandeure der jeweiligen *ASGs*, *BSBs* und andere Kommandeure sowie Mitarbeiter der für die Sicherheit und den Schutz von Einrichtungen zuständigen Stellen haben die Überprüfungen strengstens zu kontrollieren und sie vertraulich zu behandeln. Die zuständigen Kommandeure haben sicherzustellen, dass nur Personen, die Kenntnis der in den über die Überprüfungen geführten Akten erfassten Daten, haben müssen, Zugang zu diesen Akten gewährt wird (AR 381-45). Personenüberprüfungen, die ergeben, dass Eintragungen vorliegen, sind über die für die Sicherheit und den Schutz von Einrichtungen zuständigen Stellen an den für den Arbeitnehmer zuständigen Kommandeur weiterzuleiten, damit dieser weitere Massnahmen ergreifen kann. Zusätzliche Vorgaben, s. Abs. 30b(5)(b).

c. Gültigkeitsdauer der Ausweise: Befristete Kasernenausweise sind bis zu 90 Tage gültig, reguläre Kasernenausweise bis zu 5 Jahre bzw. bis zu dem Tag, an dem das für die Ausstellung des Ausweises vorgelegte Dokument (z. B. Reisepaß) seine Gültigkeit verliert. Maßgebend ist das frühere Datum.

d. Erfordernisse bzgl. eines Sponsors: Die Organisation, für die der ortsansässige Arbeitnehmer tätig wird, hat die in dieser Dienstvorschrift beschriebenen Aufgaben eines *Sponsors* wahrzunehmen.

e. Personenüberprüfungen:

(1) Polizeiliches Führungszeugnis: Ein befristeter Kasernenausweis kann nur nach Vorlage eines polizeilichen Führungszeugnisses ausgestellt werden.

(2) Überprüfung durch die US-Militärpolizei: Ein befristeter Kasernenausweis kann nur nach Abschluss dieser Überprüfung ausgestellt werden. (**ANMERKUNG:** Dies gilt nur für US-Bürger.)

(3) The Defense Clearance and Investigations Index (DCII): Wenn Antragsteller eine frühere Zugehörigkeit bzw. Verbindung zu den US-Streitkräften angeben und ihnen eine *Social Security Number* ausgestellt wurde, kann ein befristeter Kasernenausweis nur nach Abschluss dieser Überprüfung ausgestellt werden.

(4) FNS-Überprüfung: Diese Überprüfung ist sowohl für nicht-amerikanische Staatsbürger durchzuführen als auch für amerikanische Staatsbürger, die seit mehr als 12 aufeinander folgenden Monaten in Deutschland leben. Die Überprüfung ist vor Ausstellung eines befristeten Kasernenausweises in die Wege zu leiten und vor Ausstellung eines regulären Kasernenausweises abzuschließen. Nachteilige Informationen dürfen zur Ausstellung eines Kasernenausweises nicht vorliegen. Dieses Erfordernis gilt nicht, wenn der Arbeitnehmer vor dem 3. Oktober 1985 eingestellt wurde (*USAREUR-Reg 604-1*).

f. Aufenthalts- und Arbeitserlaubnis: Die Vorlage dieser Dokumente kann erforderlich sein, wenn der Antragsteller kein Bürger des Aufnahmestaates oder nicht in der Europäischen Union (EU) beheimatet ist.

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen der Ausweisinhaber Zugang erhält: Die Zugangsberechtigung ist auf die Einrichtungen zu beschränken, zu denen der Arbeitnehmer zur Durchführung seiner Aufgaben Zugang benötigt.

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Keine, es sei denn Beschränkungen sind vom *Sponsor* verfügt.

i. Beschränkungen bzgl. der Berechtigung, Personen in Besucherlisten einzutragen: Inhabern befristeter Kasernenausweise ist keine diesbezügliche Berechtigung zu gewähren; Inhabern regulärer Kasernenausweise sind diesbezügliche Rechte nur dann einzuräumen, wenn dies von der *Sponsoring Organization* begründet wird. Liegt eine Begründung von der *Sponsoring Organization* für die Berechtigung, Personen in Besucherlisten einzutragen, vor, dürfen höchstens 4 Personen mit ihren Fahrzeugen eingetragen werden und dies nur für dienstliche Zwecke. Bei Sicherheitsstufe Delta dürfen keine Besucher eingetragen werden.

j. Sicherheitsstufenbezogene Beschränkungen: In Zusammenhang mit den Sicherheitsstufen bestehen keine Zugangsbeschränkungen.

14. MITARBEITER VERPFLICHTETER PRIVATFIRMEN (IN DEN USA BEHEIMATET)

a. Definition: Hierzu zählen alle Mitarbeiter verpflichteter Privatfirmen, die in den USA leben und im Rahmen eines mit dem US-Verteidigungsministerium abgeschlossenen Vertrags im *USAREUR AOR* tätig, aber nicht im Besitz einer *DOD ID-Card* sind. Obgleich Angehörigen dieser Personengruppe ein Kasernenausweis ausgestellt werden kann, ist dieser Ausweis speziell für aus den USA stammende Mitarbeiter verpflichteter Privatfirmen bestimmt, die vorübergehend im *USAREUR AOR* tätig sind.

ANMERKUNG: Voraussetzung für die Ausstellung eines Kasernenausweises ist die vertragliche Verpflichtung durch das US-Verteidigungsministerium. Mitarbeitern verpflichteter Privatfirmen, die einen Vertrag mit dem US-Verteidigungsministerium anstreben, kann Zugang zu Einrichtungen der US-Streitkräfte nur durch Eintragung in Besucherlisten bzw. durch Aufnahme in eine Registrierungsliste gewährt werden.

b. Folgende Ausweise können ausgestellt werden. Mitarbeitern verpflichteter Privatfirmen (in den USA beheimatet) können folgende Kasernenausweise ausgestellt werden:

(1) Befristeter Kasernenausweis: Dieser Ausweis kann bei einem Aufenthalt von nicht länger als 90 Tagen ausgestellt werden.

(2) Kasernenausweis. Ein Kasernenausweis kann nur bei einem zusammenhängenden Aufenthalt im *USAREUR AOR* von mehr als 90 Tagen genehmigt werden.

c. Gültigkeitsdauer der Ausweise: Der befristete Kasernenausweis ist für die Dauer des Aufenthalts bzw. bis zu 90 Tage gültig. Maßgebend ist der kürzere Zeitraum. Der Kasernenausweis ist für die Dauer des Aufenthalts (wobei es sich um einen zusammenhängenden Aufenthalt von mehr als 90 Tagen handeln muß) gültig, für die Dauer von bis zu einem Jahr bzw. bis zu dem Tag, an dem das für die Ausstellung vorgelegte Dokument (z.B. Reisepass) seine Gültigkeit verliert. Maßgebend ist der frühere Zeitpunkt.

d. Erfordernisse bzgl. eines Sponsors: Die Organisation, für die die Mitarbeiter verpflichteter Privatfirmen im *USAREUR AOR* tätig werden bzw. die diese begleitet, hat die in dieser Dienstvorschrift beschriebenen Aufgaben eines *Sponsors* wahrzunehmen.

e. Personenüberprüfungen: Für Personen dieser Gruppe sind keine Personenüberprüfungen erforderlich.

f. Aufenthalts- und Arbeitserlaubnis: Die Vorlage einer Aufenthaltserlaubnis ist unter Umständen erforderlich (Abs. 30b(6)).

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen Zugang gewährt wird: Die Zahl der Einrichtungen, zu denen Zugang gewährt wird, ist auf die Einrichtungen zu beschränken, zu denen Mitarbeiter verpflichteter Privatfirmen zur Durchführung ihrer Aufgaben und Tätigkeiten Zugang benötigen.

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Keine, es sei denn Beschränkungen sind vom *Sponsor* verfügt.

i. Beschränkungen bzgl. der Berechtigung, Personen in Besucherlisten einzutragen: Personen dieser Gruppe ist diese Berechtigung nicht zu gewähren.

j. Sicherheitsstufenbezogene Beschränkungen: In Zusammenhang mit den Sicherheitsstufen bestehen keine Zugangsbeschränkungen.

15. MITARBEITER VERPFLICHTETER PRIVATFIRMEN (IM AUFNAHMESTAAT LEBEND)

a. Definition: Hierzu zählen alle Mitarbeiter verpflichteter Privatfirmen, die im Aufnahmestaat leben und im Rahmen eines mit dem US-Verteidigungsministerium abgeschlossenen Vertrags im *USAREUR AOR* tätig, aber nicht im Besitz einer *DOD ID-Card* sind.

ANMERKUNG: Voraussetzung für die Ausstellung eines Kasernenausweises ist die vertragliche Verpflichtung durch das US-Verteidigungsministerium. Mitarbeitern verpflichteter Privatfirmen, die einen Vertrag mit dem US-Verteidigungsministerium anstreben, kann Zugang nur durch Eintragung in Besucherlisten bzw. durch Aufnahme in eine Registrierungsliste gewährt werden.

b. Folgende Ausweise können ausgestellt werden:

(1) Befristeter Kasernenausweis: Dieser Ausweis kann nur nach Abschluss aller erforderlichen Personenüberprüfungen und Einleitung der *FNS*-Überprüfung bewilligt werden.

(2) Kasernenausweis: Kann nach Abschluss aller Personenüberprüfungen (einschl. der *FNS*-Überprüfung) mit negativem Ergebnis (ohne Eintragungen) ausgestellt werden.

ANMERKUNG: Personenüberprüfungen, die ergeben, dass Eintragungen vorliegen, sind an die *ASG*, in der der Antragsteller tätig wird, zur Entscheidung weiterzuleiten. Die Kommandeure der jeweiligen *ASGs*, *BSBs* und andere Kommandeure sowie Mitarbeiter der für die Sicherheit und den Schutz von Einrichtungen zuständigen Stellen haben die Überprüfungen strengstens zu kontrollieren und sie vertraulich zu behandeln. Die zuständigen Kommandeure haben sicherzustellen, dass nur Personen, die Kenntnis der in den über die Überprüfungen geführten Akten erfassten Daten, haben müssen, Zugang zu diesen Akten gewährt wird (AR 381-45). Personenüberprüfungen, die ergeben, dass Eintragungen vorliegen, sind über die für die Sicherheit und den Schutz von Einrichtungen zuständigen Stellen an den für den Arbeitnehmer zuständigen Kommandeur weiterzuleiten, damit dieser weitere Massnahmen ergreifen kann. Zusätzliche Vorgaben, s. Abs. 30b(5)(b).

c. Gültigkeitsdauer der Ausweise: Ein befristeter Kasernenausweis ist für die Dauer des Vertrages bzw. bis zu 90 Tage gültig. Maßgebend ist der kürzere Zeitraum. Der Kasernenausweis ist für die Dauer des Aufenthalts gültig, für die Dauer von bis zu zwei Jahren bzw. bis zu dem Tag, an dem das für die Ausstellung vorgelegte Dokument (z.B. Reisepass) seine Gültigkeit verliert. Maßgebend ist der frühere Zeitpunkt.

d. Erfordernisse bzgl. eines Sponsors:

(1) Im Gegensatz zu Personen in anderen Gruppen, kann es sein, dass die *Sponsoring Organization* für diese Gruppe von Mitarbeitern verpflichteter Privatfirmen schwieriger zu bestimmen ist. Im allgemeinen hat die Organisation, bei der Mitarbeiter einer verpflichteten Privatfirma tätig sind, die in diesem Kapitel beschriebenen Aufgaben eines *Sponsors* wahrzunehmen. Ein Zugang ist für diese Mitarbeiter von der verpflichtenden Organisation nur in dem erforderlichen Umfang zu beantragen. Für Mitarbeiter von Firmen, die z. B. im Auftrag einer Organisation Möbel in zwei Einrichtungen innerhalb eines *BSB* anliefern, ist die Ausstellung eines gültigen Kasernenausweises für Zugang, der über die *BSB* hinaus geht, nicht zu beantragen und zu befürworten.

(2) Folgende Erfordernisse hinsichtlich *Sponsoring Organization* gelten für unterschiedliche Zugangsstufen:

(a) Wenn Zugang zu mehr als drei *ASGs* beantragt wird, wird der Antrag wie ein Antrag auf „*USAREUR*-weiten“ Zugang betrachtet. Im Einzelnen können Anträge für den Zugang zu mehr als drei *ASGs* nur durch folgende Dienststellen, die die Aufgaben der *Sponsoring Organization* übernehmen, genehmigt werden:

1. *Department of Defense Dependents Schools-Europe*
2. *Defense Commissary Agency, European Region*
3. *Defense Logistics Agency, Europe*
4. *Army and Air Force Exchange Service, Europe (AAFES-Eur)*
5. *Military Surface Deployment and Distribution Command, Europe*
6. *United States Army Center for Health Promotion and Preventive Medicine - Europe*
7. *United States Army Medical Materiel Center, Europe*
8. *United States Army Corps of Engineers, Europe District*
9. *IMA-E*
10. *HQ USAREUR/7A, Stabsabteilungen*
11. *V Corps*
12. *21st Theater Support Command*
13. *United States Army Southern European Task Force*
14. *Seventh Army Training Command*
15. *7th Army Reserve Command*
16. *266th Finance Command*
17. *1st Personnel Command*
18. *18th Engineer Brigade*
19. *5th Signal Command*
20. *66th Military Intelligence Group*
21. *202d Military Police Group*
22. *United States Army Europe Regional Medical Command*
23. *United States Army Europe Regional Dental Command*

24. United States Army Contracting Command, Europe

25. United States Army Materiel Command, Europe

26. 1st Theater Movement Control Agency

ANMERKUNG: Die Entscheidung über Fälle, in denen eine Organisation, die nicht oben aufgeführt ist, der Meinung ist, sie sollte als *Sponsoring Organization* für USAREUR-weiten Zugang fungieren können, liegt beim *USAREUR PM*.

(b) Wenn Zugang zu zwei oder drei ASGs benötigt wird, finden die Anforderungen an Rang/Gehaltsgruppe von Absatz 30b(2)(c) Anwendung; die *Sponsoring Organization* muss jedoch keine der in (a) oben aufgeführten Dienststellen sein. Die *Sponsoring Organization* ist die ASG, in der die Vertragsfirma ihren Sitz hat oder der Mitarbeiter den wesentlichen Teil der Arbeit erledigt.

(c) Mitarbeiter verpflichteter Vertragsfirmen, deren Dienste mehrere BSBs umfassen, aber auf eine ASG beschränkt sind, können einen Kasernenausweis für die ASG erhalten. Die ASG muss die *Sponsoring Organization* sein.

(d) In allen anderen Fällen haben die *Sponsoring Organizations* keine Vollmacht, Antragsteller über die BSB hinaus zu sponsern.

(3) Mitarbeiter verpflichteter Vertragsfirmen, die aufgrund der in (2) oben aufgelisteten Voraussetzungen keinen Kasernenausweis erhalten können, aber auf Grundlage einzelner Verträge mit unterschiedlichen Organisationen Zugang zu Einrichtungen im *USAREUR AOR* brauchen, sollten einen Kasernenausweis für die ASG oder BSB erhalten, wo sie den Großteil ihrer Arbeit erledigen und für andere Orte die Einschreibeverfahren oder die spezifischen Zugangslisten der jeweiligen Einrichtung nutzen. Absatz 42 enthält Voraussetzungen für Mitarbeiter verpflichteter Vertragsfirmen hinsichtlich Zugangslisten.

e. Personenüberprüfungen:

(1) **Polizeiliches Führungszeugnis:** Ein befristeter Kasernenausweis oder ein Kasernenausweis kann nur nach Vorlage eines polizeilichen Führungszeugnisses ausgestellt werden.

(2) **Überprüfung durch die US-Militärpolizei:** Ein befristeter Kasernenausweis oder ein Kasernenausweis kann nur nach Abschluss dieser Überprüfung ausgestellt werden. (**ANMERKUNG:** Dies gilt nur für US-Bürger.)

(3) **DCII-Überprüfung:** Wenn Antragsteller eine frühere Zugehörigkeit bzw. Verbindung zu den US-Streitkräften angeben und ihnen eine *Social Security Number* ausgestellt wurde, kann ein befristeter Kasernenausweis oder ein Kasernenausweis nur nach Abschluss dieser Überprüfung ausgestellt werden.

(4) **FNS-Überprüfung:** Diese Überprüfung ist sowohl für nicht-amerikanische Staatsbürger durchzuführen als auch für amerikanische Staatsbürger, die seit mehr als 12 aufeinander folgenden Monaten in Deutschland leben. Die Überprüfung ist vor Ausstellung eines befristeten Kasernenausweises in die Wege zu leiten und vor Ausstellung eines regulären Kasernenausweises abzuschließen. Nachteilige Informationen dürfen zur Ausstellung eines Kasernenausweises nicht vorliegen.

f. Aufenthalts- und Arbeitserlaubnis: Diese Genehmigungen können von nicht-deutschen Staatsbürgern verlangt werden, soweit der nicht-deutsche Staatsbürger von dieser Voraussetzung nicht befreit ist (Abs. 30b(6)(d)).

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen der Ausweisinhaber Zugang erhält: Die Zugangsberechtigung ist auf die Einrichtungen zu beschränken, zu denen Mitarbeiter verpflichteter Privatfirmen zur Durchführung ihrer Aufgaben unbedingt Zugang brauchen (s. vorstehenden Abs. d).

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Keine, es sei denn Beschränkungen sind vom *Sponsor* verfügt.

i. Beschränkungen bzgl. der Eintragung von Personen in Besucherlisten: Mitarbeiter verpflichteter Privatfirmen sind in der Regel nicht berechtigt, Personen in Besucherlisten einzutragen. Ausnahmen sind zulässig, wenn der *Sponsoring Official* mindestens den Rang eines *Lieutenant Colonel* (Oberstleutnant) hat oder als Zivilbediensteter als *GS-13* oder *C-8* oder höher eingruppiert ist. Die *22d* und *80th ASG* können hier für ihre ortsansässigen Arbeitnehmer die entsprechenden Eingruppierungsstufen zugrunde legen. Die Berechtigung zum Eintragen von Besuchern in Besucherlisten gilt nicht bei Sicherheitsstufe Delta und ist auf das Eintragen von vier Personen mit Fahrzeugen beschränkt. Nur andere Mitarbeiter verpflichteter Privatfirmen bzw. Händler und Dienstleister können zur Erfüllung des Vertrags eingetragen werden. Inhabern eines befristeten Kasernenausweises ist keine Berechtigung zum Eintragen von Personen in Besucherlisten einzuräumen.

j. Sicherheitsstufenbezogene Beschränkungen: Der befristete Kasernenausweis berechtigt zum Zugang bei Sicherheitsstufe Alpha und Sicherheitsstufe Bravo. Eine einstufige Erweiterung der Zugangsberechtigung kann auf Antrag der *Sponsoring Organization* durch das *IACO* gewährt werden. Für den Kasernenausweis gelten keine Beschränkungen.

16. HAUSANGESTELLTE

a. Definition: Hierunter fallen alle Personen, die von der beantragenden Person (s. Glossar) zur Durchführung einer Dienstleistung verpflichtet werden (z. B. als Kinderfrau, Hundebetreuer, Reinigungspersonal).

b. Folgende Ausweise können ausgestellt werden:

(1) Befristeter Kasernenausweis: Dieser Ausweis wird nach Abschluss aller Personenüberprüfungen, mit Ausnahme der *FNS*-Überprüfung, ausgestellt.

(2) Kasernenausweis: Kann nach Abschluss aller Personenüberprüfungen (einschl. der *FNS*-Überprüfung) mit negativem Ergebnis (ohne Eintragungen) ausgestellt werden.

ANMERKUNG: Personenüberprüfungen, die ergeben, dass Eintragungen vorliegen, sind an die *ASG*, in der der Antragsteller tätig wird, zur Entscheidung weiterzuleiten. Die Kommandeure der jeweiligen *ASGs*, *BSBs* und andere Kommandeure sowie Mitarbeiter der für die Sicherheit und den Schutz von Einrichtungen zuständigen Stellen haben die Überprüfungen strengstens zu kontrollieren und sie vertraulich zu behandeln. Die zuständigen Kommandeure haben sicherzustellen, dass nur Personen, die Kenntnis der in den über die Überprüfungen geführten Akten erfassten Daten, haben müssen, Zugang zu diesen Akten gewährt wird (AR 381-45). Personenüberprüfungen, die ergeben, dass Eintragungen vorliegen, sind über die für die Sicherheit und den Schutz von Einrichtungen zuständigen Stellen an den für den Arbeitnehmer zuständigen Kommandeur weiterzuleiten, damit dieser weitere Massnahmen ergreifen kann. Zusätzliche Vorgaben, s. Abs. 30b(5)(b).

c. Gültigkeitsdauer der Ausweise: Der befristete Kasernenausweis ist für die Dauer der Verpflichtung bzw. bis zu 90 Tage gültig. Maßgebend ist der kürzere Zeitraum. Der Kasernenausweis ist für die Dauer der Verpflichtung, für 2 Jahre oder bis zu dem Tag, an dem das für die Ausstellung vorgelegte Dokument (z. B. Reisepaß) seine Gültigkeit verliert, gültig. Maßgebend ist der kürzere Zeitraum.

d. Erfordernisse bzgl. eines Sponsors: Das *BSB*, in dem die beantragende Person ihren Wohnsitz hat, übernimmt die Funktion des *Sponsors* für diese Person und nimmt die Aufgaben eines *Sponsors* wahr.

e. Personenüberprüfungen:

(1) Polizeiliches Führungszeugnis: Ein befristeter Kasernenausweis oder ein Kasernenausweis kann nur nach Vorlage eines polizeilichen Führungszeugnisses ausgestellt werden.

(2) Überprüfung durch die US-Militärpolizei: Ein befristeter Kasernenausweis oder ein Kasernenausweis kann nur nach Abschluss dieser Überprüfung ausgestellt werden. (**ANMERKUNG:** Dies gilt nur für US-Bürger.)

(3) DCII-Überprüfung: Wenn Antragsteller eine frühere Zugehörigkeit bzw. Verbindung zu den US-Streitkräften angeben und ihnen eine *Social Security Number* ausgestellt wurde, kann ein befristeter Kasernenausweis oder ein Kasernenausweis nur nach Abschluss dieser Überprüfung ausgestellt werden.

(4) FNS-Überprüfung: Diese Überprüfung ist sowohl für nicht-amerikanische Staatsbürger durchzuführen als auch für amerikanische Staatsbürger, die seit mehr als 12 aufeinander folgenden Monaten in Deutschland leben. Die Überprüfung ist vor Ausstellung eines befristeten Kasernenausweises in die Wege zu leiten und vor Ausstellung eines regulären Kasernenausweises abzuschließen. Nachteilige Informationen dürfen zur Ausstellung eines Kasernenausweises nicht vorliegen.

f. Aufenthalts- und Arbeitserlaubnis: Diese Genehmigungen können von nicht-deutschen Staatsbürgern verlangt werden, soweit der nicht-deutsche Staatsbürger von dieser Voraussetzung nicht befreit ist (Abs. 30b(6)(d)).

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen Zugang gewährt wird: Der Zugang darf das *BSB*, das die Aufgaben eines *Sponsors* übernimmt, nicht überschreiten. Dieses *BSB* kann den Zugang nach Bedarf weiter einschränken. Die Zugangsberechtigung kann auf die *ASG* erweitert werden, wenn die *ASG* bereit ist, die Aufgaben der *Sponsoring Organization* wahrzunehmen.

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Keine, es sei denn die beantragende Person bzw. der *Sponsor* verfügen Beschränkungen.

i. Beschränkungen bzgl. der Eintragung von Personen in Besucherlisten: Personen dieser Gruppe ist diese Berechtigung nicht zu gewähren.

j. Sicherheitsstufenbezogene Beschränkungen: Der befristete Kasernenausweis berechtigt zum Zugang bei Sicherheitsstufe Alpha und Sicherheitsstufe Bravo. Eine einstufige Erweiterung der Zugangsberechtigung kann auf Antrag der *Sponsoring Organization* durch das *IACO* gewährt werden. Für Kasernenausweise gelten keine Beschränkungen.

17. ZULIEFERER (REGELMÄßIGE ANLIEFERUNGEN ODER ÄHNLICHE DIENSTLEISTUNGEN, DIE NICHT IN VERBINDUNG MIT EINEM MIT DER US-REGIERUNG ABGESCHLOSSENEN VERTRAG ERBRACHT WERDEN)

a. Definition: Hierunter fallen Personen, die aufgrund einer bestehenden Verpflichtung wiederholt zur Anlieferung von Waren oder zum Erbringen ähnlicher Dienstleistungen in Verbindung mit ihrer Arbeit Zugang zu Einrichtungen der US-Streitkräfte benötigen (z. B.: Pizza- und Taxiservice).

b. Folgende Ausweise können ausgestellt werden:

(1) Befristeter Kasernenausweis: Dieser Pass kann nicht ausgestellt werden.

(2) Kasernenausweis: Kann nach Abschluss aller Personentüberprüfungen (einschl. der *FNS*-Überprüfung) mit negativem Ergebnis (ohne Eintragungen) ausgestellt werden.

ANMERKUNG: Personenüberprüfungen, die ergeben, dass Eintragungen vorliegen, sind an die *ASG*, in der der Antragsteller tätig wird, zur Entscheidung weiterzuleiten. Die Kommandeure der jeweiligen *ASGs*, *BSBs* und andere Kommandeure sowie Mitarbeiter der für die Sicherheit und den Schutz von Einrichtungen zuständigen Stellen haben die Überprüfungen strengstens zu kontrollieren und sie vertraulich zu behandeln. Die zuständigen Kommandeure haben sicherzustellen, dass nur Personen, die Kenntnis der in den über die Überprüfungen geführten Akten erfassten Daten, haben müssen, Zugang zu diesen Akten gewährt wird (AR 381-45). Personenüberprüfungen, die ergeben, dass Eintragungen vorliegen, sind über die für die Sicherheit und den Schutz von Einrichtungen zuständigen Stellen an den für den Arbeitnehmer zuständigen Kommandeur weiterzuleiten, damit dieser weitere Massnahmen ergreifen kann. Zusätzliche Vorgaben, s. Abs. 30b(5)(b).

c. Gültigkeitsdauer des Ausweises: Der Kasernenausweis ist 2 Jahre lang gültig oder läuft mit Ablauf der Gültigkeit des für die Ausstellung vorgelegten Dokuments (z. B. Reisepass) ab. Maßgebend ist der kürzere Zeitraum.

d. Erfordernisse bzgl. eines *Sponsors*: Das *BSB*, für das die Dienstleistung erbracht wird, fungiert für Personen in dieser Gruppe als *Sponsor*.

e. Personenüberprüfungen:

(1) Polizeiliches Führungszeugnis: Ein Kasernenausweis kann nur nach Vorlage eines polizeilichen Führungszeugnisses ausgestellt werden.

(2) Überprüfung durch die US-Militärpolizei: Ein Kasernenausweis kann nur nach Abschluss dieser Überprüfung ausgestellt werden. (**ANMERKUNG:** Dies gilt nur für US-Bürger.)

(3) *DCII*-Überprüfung: Wenn Antragsteller eine frühere Zugehörigkeit bzw. Verbindung zu den US-Streitkräften angeben und ihnen eine *Social Security Number* ausgestellt wurde, kann ein Kasernenausweis nur nach Abschluss dieser Überprüfung ausgestellt werden.

(4) FNS-Überprüfung: Diese Überprüfung ist sowohl für nicht-amerikanische Staatsbürger durchzuführen als auch für amerikanische Staatsbürger, die seit mehr als 12 aufeinander folgenden Monaten in Deutschland leben. Die Überprüfung ist vor Ausstellung eines regulären Kasernenausweises abzuschließen. Nachteilige Informationen dürfen zur Ausstellung eines Kasernenausweises nicht vorliegen.

f. Aufenthalts- und Arbeitserlaubnis: Diese Genehmigungen sind von nicht-deutschen Staatsbürgern vorzulegen. Abs. 30b(6)(d) erläutert Ausnahmen zu dieser Regelung.

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen Zugang gewährt wird: Inhabern von Kasernenausweisen ist Zugang nur in dem *BSB* zu gewähren, das als *Sponsor* fungiert. Die Zugangsberechtigung kann von diesem *BSB* gegebenenfalls weiter eingeschränkt werden (z.B. nur auf bestimmte Kasernen). Die Zugangsberechtigung kann nur auf die *ASG* erweitert werden, wenn die *ASG* bereit ist, die Aufgaben der *Sponsoring Organization* wahrzunehmen.

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Keine, es sei denn der *Sponsor* hat Beschränkungen bestimmt.

i. Beschränkungen bzgl. der Eintragung von Personen in Besucherlisten: Personen dieser Gruppe ist diese Berechtigung nicht zu gewähren.

j. Sicherheitsstufenbezogene Beschränkungen: Eine Zugangsberechtigung unter Vorlage eines Kasernenausweises besteht nur bei Sicherheitsstufe Alpha und Bravo. Eine einstufige Erweiterung der Zugangsberechtigung kann auf Antrag der *Sponsoring Organization* durch das *IACO* gewährt werden.

18. HÄNDLER UND DIENSTLEISTER

a. Definition: Hierzu zählen alle Personen, die berechtigt sind, in Einrichtungen der US-Streitkräfte Waren zu verkaufen oder Dienstleistungen zu erbringen.

b. Folgende Ausweise können ausgestellt werden:

(1) Befristeter Kasernenausweis: Dieser Pass kann nicht ausgestellt werden.

(2) Kasernenausweis: Kann nach Abschluss aller Personenüberprüfungen (einschl. der *FNS*-Überprüfung) mit negativem Ergebnis (ohne Eintragungen) ausgestellt werden.

ANMERKUNG: Personenüberprüfungen, die ergeben, dass Eintragungen vorliegen, sind an die *ASG*, in der der Antragsteller tätig wird, zur Entscheidung weiterzuleiten. Die Kommandeure der jeweiligen *ASGs*, *BSBs* und andere Kommandeure sowie Mitarbeiter der für die Sicherheit und den Schutz von Einrichtungen zuständigen Stellen haben die Überprüfungen strengstens zu kontrollieren und sie vertraulich zu behandeln. Die zuständigen Kommandeure haben sicherzustellen, dass nur Personen, die Kenntnis der in den über die Überprüfungen geführten Akten erfassten Daten, haben müssen, Zugang zu diesen Akten gewährt wird (AR 381-45). Personenüberprüfungen, die ergeben, dass Eintragungen vorliegen, sind über die für die Sicherheit und den Schutz von Einrichtungen zuständigen Stellen an den für den Arbeitnehmer zuständigen Kommandeur weiterzuleiten, damit dieser weitere Massnahmen ergreifen kann. Zusätzliche Vorgaben, s. Abs. 30b(5)(b).

c. Gültigkeitsdauer des Ausweises: Die Gültigkeitsdauer des Ausweises ist auf 2 Jahre begrenzt bzw. auf die Gültigkeitsdauer des für die Ausstellung vorgelegten Dokuments (z. B. Reisepass) oder auf die Gültigkeitsdauer der ausgestellten Lizenz bzw. des Gewerbescheins. Maßgebend ist der kürzere Zeitraum.

d. Erfordernisse bzgl. eines Sponsors: Das *BSB* fungiert als *Sponsoring Organization*, wenn der beantragte Zugang das *BSB* nicht überschreitet. Die *ASG* fungiert als *Sponsoring Organization*, wenn der beantragte Zugang ein *BSB* überschreitet, aber auf eine *ASG* beschränkt ist. Bei Zugang zu mehr als einer *ASG* muss der Antragsteller von *AAFES-Eur*, *Defense Commissary Agency*, *European Region*, oder *IMA-E* gesponsort werden. Diese Berechtigung zur Übernahme der Sponsorfunktion darf nicht an nachgeordnete Organisationen übertragen werden.

e. Personenüberprüfungen:

(1) Polizeiliches Führungszeugnis: Ein Kasernenausweis kann nur nach Vorlage eines polizeilichen Führungszeugnisses ausgestellt werden.

(2) **Überprüfung durch die US-Militärpolizei:** Ein Kasernenausweis kann nur nach Abschluss dieser Überprüfung ausgestellt werden. (ANMERKUNG: Dies gilt nur für US-Bürger.)

(3) **DCII-Überprüfung:** Wenn Antragsteller eine frühere Zugehörigkeit bzw. Verbindung zu den US-Streitkräften angeben und ihnen eine *Social Security Number* ausgestellt wurde, kann ein Kasernenausweis nur nach Abschluss dieser Überprüfung ausgestellt werden.

(4) **FNS-Überprüfung:** Diese Überprüfung ist sowohl für nicht-amerikanische Staatsbürger durchzuführen als auch für amerikanische Staatsbürger, die seit mehr als 12 aufeinander folgenden Monaten in Deutschland leben. Die Überprüfung ist vor Ausstellung eines regulären Kasernenausweises abzuschließen. Nachteilige Informationen dürfen zur Ausstellung eines Kasernenausweises nicht vorliegen.

f. Aufenthalts- und Arbeitserlaubnis: Diese Genehmigungen werden von nicht-deutschen Staatsbürgern verlangt, soweit der nicht-deutsche Staatsbürger von dieser Voraussetzung nicht befreit ist (Abs. 30b(6)(d)).

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen Zugang gewährt wird: Die Anzahl der Einrichtungen, zu denen einem Inhaber eines Kasernenausweises Zugang gewährt werden kann, hängt von der Stufe der *Sponsoring Organization* ab (d oben).

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Keine, es sei denn der *Sponsor* hat Beschränkungen bestimmt.

i. Beschränkungen bzgl. der Eintragung von Personen in Besucherlisten: Personen dieser Gruppe ist diese Berechtigung nicht zu gewähren.

j. Sicherheitsstufenbezogene Beschränkungen: Eine Zugangsberechtigung unter Vorlage eines Kasernenausweises besteht nur bei Sicherheitsstufe Alpha und Bravo. Eine einstufige Erweiterung der Zugangsberechtigung kann auf Antrag der *Sponsoring Organization* durch das *IACO* gewährt werden.

19. NATO-ANGEHÖRIGE

a. Definition: Hierzu zählen alle Militär- und Zivilangehörigen der NATO mit ihren Familien, die ihren Wohnsitz in Deutschland haben oder die in *USAREUR-Regulation 600-700* aufgestellten Voraussetzungen erfüllen. Diese Gruppe ist für Vertreter von NATO-Entsendestaaten (aktive belgische, britische, kanadische, niederländische und französische Militärangehörige, die in Deutschland stationiert sind) vorgesehen und sollte nicht mit der Gruppe der Militärangehörigen aus dem Aufnahmestaat in Abs. 20 verwechselt werden.

b. Folgende Ausweise können ausgestellt werden:

(1) **Befristeter Kasernenausweis:** Dieser Ausweis kann nicht ausgestellt werden.

(2) **Kasernenausweis:** Dieser Ausweis kann ausgestellt werden.

c. Gültigkeitsdauer des Ausweises: Die Gültigkeitsdauer des Kasernenausweises ist auf 5 Jahre begrenzt, auf die Dauer der jeweiligen Dienstzeit bzw. bis zum Ablauf der Gültigkeitsdauer des für die Ausstellung vorgelegten Dokuments (z. B. Militärausweis). Maßgebend ist der kürzere Zeitraum.

d. Erfordernisse bzgl. eines Sponsors:

(1) **Angehörige der NATO, die in Deutschland einem internationalen Militärhauptquartier unterstellt oder mit einer Sonderaufgabe bzw. mit einem Sonderauftrag betraut sind:** Für Personen in dieser Gruppe fungiert die vorgesetzte Dienststelle als *Sponsor*.

(2) **Militärangehörige (aktiver Dienst) der in Deutschland stationierten Streitkräfte Belgiens, Großbritannien, Kanadas, der Niederlande und Frankreichs (auch als Entsendestaaten bezeichnet):** Das Sicherheitsbüro des Entsendestaates fungiert als *Sponsor* für Personen in dieser Gruppe. Die bestellten *Sponsoring Officials* sind dem *USAREUR PM* von dem Entsendestaat per E-Mail mitzuteilen (*iacs@manupo.pmo.army.mil*). Der *USAREUR PM* hat die Liste auf dem mit einer Zugangsbeschränkung versehenen Teil der *IACS*-Webseite zu veröffentlichen, wo sie allen *IACOs* von *USAREUR* zugänglich ist. Personen, die dieser Gruppe zuzurechnen sind, können sich in jedem *IACO* einen Kasernenausweis ausstellen lassen. Da diese Personen in ganz Deutschland stationiert sind, ist der erste Besuch einer von den US-Streitkräften kontrollierten Einrichtung mit der *Sponsoring Organization* und dem *IACO* zur Ausstellung eines Kasernenausweises gemäß Abs. 30c abzustimmen.

(3) Angehörige des französischen und britischen konsularischen und diplomatischen Dienstes in Deutschland:

Die *U.S. Mission, Germany (U.S. Department of State)* fungiert als *Sponsor* für Personen in dieser Gruppe. Die bestellten *Sponsoring Officials* sind dem *USAREUR PM* von der *U.S. Mission, Germany*, per E-Mail mitzuteilen. Der *USAREUR PM* hat die Liste auf dem mit einer Zugangsbeschränkung versehenen Teil der *IACS*-Webseite zu veröffentlichen, wo sie allen *IACOs* von *USAREUR* zugänglich ist. Personen, die dieser Gruppe zuzurechnen sind, können sich in jedem *IACO* einen Kasernenausweis ausstellen lassen. Der erste Besuch von Angehörigen des französischen und britischen konsularischen und diplomatischen Dienstes in einer von den US-Streitkräften kontrollierten Einrichtung ist mit der *Sponsoring Organization* und dem *IACO* zur Ausstellung eines Kasernenausweises gemäß Abs. 30c abzustimmen.

e. Personenüberprüfungen: Personenüberprüfungen sind für Personen in dieser Gruppe nicht erforderlich.

f. Aufenthalts- und Arbeitserlaubnis: Personen in dieser Gruppe benötigen keine Aufenthalts- oder Arbeitserlaubnisse.

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen Zugang gewährt wird: Es gelten keine Beschränkungen. Angehörigen der NATO wird automatisch Zugang zu allen Einrichtungen der US-Streitkräfte gewährt. Eine Begründung ist hierfür nicht erforderlich.

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Es gibt keine Beschränkungen darüber, wann Zugang gewährt werden kann.

i. Beschränkungen bzgl. der Eintragung von Personen in Besucherlisten: Personen in dieser Gruppe können nur vier Personen mit Fahrzeugen in Besucherlisten eintragen.

j. Sicherheitsstufenbezogene Beschränkungen: Bezüglich der Sicherheitsstufen gelten keine Beschränkungen.

20. MILITÄRANGEHÖRIGE DES AUFNAHMESTAATES

a. Definition: Hierzu zählen alle Angehörigen des Militärs des Aufnahmestaates, die in einer von den US-Streitkräften kontrollierten Einrichtung in dem Land, dem sie dienen, arbeiten oder wohnhaft sind (z.B. deutsche Soldaten in Deutschland, italienische Soldaten in Italien). Diese Gruppe sollte nicht mit der Gruppe der NATO-Angehörigen (Abs. 19) verwechselt werden, die speziell für Angehörige von NATO-Entsendestaaten (aktive belgische, britische, kanadische, niederländische und französische Militärangehörige, die in Deutschland stationiert sind) vorgesehen ist.

b. Folgende Ausweise können ausgestellt werden:

(1) Befristeter Kasernenausweis: Für Personen in dieser Gruppe sind befristete Kasernenausweise nicht zutreffend.

(2) Kasernenausweis: Personen in dieser Gruppe wird ein Kasernenausweis ausgestellt.

c. Gültigkeitsdauer des Ausweises: Die Gültigkeitsdauer der Kasernenausweise für Militärangehörige des Aufnahmestaates ist auf 5 Jahre begrenzt, auf die Dauer der jeweiligen Dienstzeit oder bis zum Ablauf der Gültigkeitsdauer des für die Ausstellung vorgelegten Dokuments (z.B. Militärausweis). Maßgebend ist der kürzere Zeitraum.

d. Erfordernisse bzgl. eines Sponsors: Wenn der Militärangehörige des Aufnahmestaates für eine Organisation mit einem *DOD*-Vertreter arbeitet, fungiert diese Organisation als *Sponsoring Organization* und übernimmt die Aufgaben eines *Sponsors*. Ist keine derartige Organisation vorhanden, übernimmt das *BSB* die Aufgaben des *Sponsors*.

e. Personenüberprüfungen: Personenüberprüfungen sind für Personen in dieser Gruppe nicht erforderlich.

f. Aufenthalts- und Arbeitserlaubnis: Personen in dieser Gruppe benötigen keine Aufenthalts- oder Arbeitserlaubnisse.

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen Zugang gewährt wird: Die Anzahl der Einrichtungen, zu denen einem Inhaber eines Kasernenausweises Zugang gewährt werden kann, ist auf Grundlage der Umstände des Militärangehörigen des Aufnahmestaates auf das erforderliche Minimum zu beschränken.

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Es gibt keine Beschränkungen darüber, wann Zugang gewährt werden kann, soweit nicht vom *Sponsor* angegeben.

i. Beschränkungen bzgl. der Eintragung von Personen in Besucherlisten: Inhaber von Kasernenausweisen sind nicht berechtigt, Personen in Besucherlisten einzutragen, es sei denn, diese Berechtigung wird von der *Sponsoring Organization* begründet. Wenn die Berechtigung zum Eintragen von Personen in Besucherlisten von der *Sponsoring Organization* begründet wird, kann der Inhaber eines Kasernenausweises bis zu vier Personen und ihre Fahrzeuge „ausschließlich für dienstliche Zwecke“ eintragen. Bei Sicherheitsstufe Delta ist der Inhaber eines Kasernenausweises nicht berechtigt, Personen in Besucherlisten einzutragen.

j. Sicherheitsstufenbezogene Beschränkungen: Bezüglich der Sicherheitsstufen gelten keine Beschränkungen.

21. AUSLÄNDISCHE LEHRGANGSTEILNEHMER (*MARSHALL CENTER*)

a. Definition: Hierzu zählen alle Angehörigen ausländischer Streitkräfte, die zur Lehrgangsteilnahme an das *George C. Marshall European Center for Security Studies* in Garmisch abkommandiert sind.

b. Folgende Ausweise können ausgestellt werden:

(1) **Befristeter Kasernenausweis:** Dieser Ausweis kann nicht ausgestellt werden.

(2) **Kasernenausweis:** Dieser Ausweis kann Personen in dieser Gruppe ausgestellt werden.

c. Gültigkeitsdauer des Ausweises: Die Gültigkeitsdauer des Ausweises ist auf 2 Jahre bzw. auf die Dauer der Abkommandierung oder bis zum Ablauf der Gültigkeitsdauer des für die Ausstellung vorgelegten Dokuments (z. B. Militärausweis) begrenzt. Maßgebend ist der kürzere Zeitraum.

d. Erfordernisse bzgl. eines Sponsors: Vertreter des *Marshall Center* übernehmen die Aufgaben eines *Sponsors*.

e. Personenüberprüfungen: Personenüberprüfungen sind für Personen in dieser Gruppe nicht erforderlich.

f. Aufenthalts- und Arbeitserlaubnis: Personen in dieser Gruppe benötigen keine Aufenthalts- oder Arbeitsgenehmigungen.

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen Zugang gewährt wird: Der Zugang ist auf das *AST Garmisch* zu beschränken.

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Es gibt keine Beschränkungen darüber, wann Zugang gewährt werden kann.

i. Beschränkungen bzgl. der Eintragung von Personen in Besucherlisten: Personen dieser Gruppe ist diese Berechtigung nicht zu gewähren.

j. Sicherheitsstufenbezogene Beschränkungen: Bezüglich der Sicherheitsstufen gelten keine Beschränkungen.

22. MITGLIEDER PRIVATER ORGANISATIONEN

a. Definition: Hierzu zählen Mitglieder genehmigter privater Organisationen, die ausschließlich zur Teilnahme an offiziellen Veranstaltungen dieser Organisationen Zugang zu Einrichtungen der US-Streitkräfte brauchen.

b. Folgende Ausweise können ausgestellt werden:

(1) **Befristeter Kasernenausweis:** Dieser Ausweis kann nicht ausgestellt werden.

(2) **Kasernenausweis:** Kann nach Abschluss aller Personenüberprüfungen (einschl. der *FNS*-Überprüfung) mit negativem Ergebnis (ohne Eintragungen) ausgestellt werden.

ANMERKUNG: Personenüberprüfungen, die ergeben, dass Eintragungen vorliegen, sind an die *ASG*, in der der Antragsteller tätig wird, zur Entscheidung weiterzuleiten. Die Kommandeure der jeweiligen *ASGs*, *BSBs* und andere Kommandeure sowie Mitarbeiter der für die Sicherheit und den Schutz von Einrichtungen zuständigen Stellen haben die Überprüfungen strengstens zu kontrollieren und sie vertraulich zu behandeln. Die zuständigen Kommandeure haben sicherzustellen, dass nur Personen, die Kenntnis der in den über die Überprüfungen geführten Akten erfassten Daten, haben müssen, Zugang zu diesen Akten gewährt wird (AR 381-45). Personenüberprüfungen, die ergeben, dass Eintragungen vorliegen, sind über die für die Sicherheit und den Schutz von Einrichtungen zuständigen Stellen an den für den Arbeitnehmer zuständigen Kommandeur weiterzuleiten, damit dieser weitere Massnahmen ergreifen kann. Zusätzliche Vorgaben, s. Abs. 30b(5)(b).

c. Gültigkeitsdauer des Ausweises: Die Gültigkeitsdauer des Ausweises ist auf 2 Jahre begrenzt bzw. bis zum Ablauf der Gültigkeitsdauer des für die Ausstellung vorgelegten Dokuments (z. B. Reisepass). Maßgebend ist der kürzere Zeitraum.

d. Erfordernisse bzgl. eines Sponsors: Das *BSB*, in dem die Veranstaltung stattfindet, übernimmt die Aufgaben des Sponsors.

e. Personenüberprüfungen:

(1) Polizeiliches Führungszeugnis: Ein Kasernenausweis kann nur nach Vorlage eines polizeilichen Führungszeugnisses ausgestellt werden.

(2) Überprüfung durch die US-Militärpolizei: Ein Kasernenausweis kann nur nach Abschluss dieser Überprüfung ausgestellt werden. (**ANMERKUNG:** Dies gilt nur für US-Bürger.)

(3) DCII-Überprüfung: Wenn Antragsteller eine frühere Zugehörigkeit bzw. Verbindung zu den US-Streitkräften angeben und ihnen eine *Social Security Number* ausgestellt wurde, kann ein Kasernenausweis nur nach Abschluss dieser Überprüfung ausgestellt werden.

(4) FNS-Überprüfung: Diese Überprüfung ist sowohl für nicht-amerikanische Staatsbürger durchzuführen als auch für amerikanische Staatsbürger, die seit mehr als 12 aufeinander folgenden Monaten in Deutschland leben. Die Überprüfung ist vor Ausstellung eines regulären Kasernenausweises abzuschließen. Nachteilige Informationen dürfen zur Ausstellung eines Kasernenausweises nicht vorliegen.

f. Aufenthalts- und Arbeitserlaubnis: Personen in dieser Gruppe benötigen keine Aufenthalts- oder Arbeitserlaubnisse.

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen Zugang gewährt wird: Der Zugang ist auf das *BSB* zu beschränken, das als *Sponsor* fungiert. Die Zugangsberechtigung kann von diesem *BSB* weiter eingeschränkt werden. Die Zugangsberechtigung kann auf die *ASG* ausgedehnt werden, wenn diese bereit ist, die Aufgaben der *Sponsoring Organization* wahrzunehmen.

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Keine, es sei denn das als *Sponsor* fungierende *BSB* verfügt Beschränkungen.

i. Beschränkungen bzgl. der Eintragung von Personen in Besucherlisten: Personen dieser Gruppe ist diese Berechtigung nicht zu gewähren.

j. Sicherheitsstufenbezogene Beschränkungen: Eine Zugangsberechtigung unter Vorlage von Kasernenausweisen besteht nur bei Sicherheitsstufe Alpha und Bravo. Eine einstufige Erweiterung der Zugangsberechtigung kann auf Antrag der *Sponsoring Organization* durch das *IACO* gewährt werden.

23. BESUCHER (DIREKTE FAMILIENANGEHÖRIGE, IN EUROPA LEBEND)

a. Definition: Hierzu zählen Personen, die 10 Jahre und älter sind, in einem direkten Verwandtschaftsverhältnis zu der beantragenden Person (Glossar) stehen und in Europa leben. In Zusammenhang mit dieser Vorschrift zählen zu den direkten Familienangehörigen folgende Verwandte der beantragenden Person: Sohn, Tochter, Mutter, Vater, Bruder, Schwester, Schwiegermutter, Schwiegervater, Schwager, Schwägerin, eigene Großeltern sowie Großeltern des Ehepartners.

b. Folgende Ausweise können ausgestellt werden:

(1) Befristeter Kasernenausweis: Dieser Ausweis kann nicht ausgestellt werden.

(2) Kasernenausweis: Dieser Ausweis kann nur ausgestellt werden, wenn die beantragende Person in einer bewachten Einrichtung wohnt.

c. Gültigkeitsdauer des Ausweises: Die Gültigkeitsdauer des Ausweises ist auf die Gültigkeitsdauer der ID-Card des beantragenden Person bzw. der Gültigkeitsdauer des für die Ausstellung vorgelegten Dokuments (z.B. Reisepass) begrenzt. Maßgebend ist der kürzere Zeitraum.

d. Erfordernisse bzgl. eines Sponsors: Das *BSB*, in dem die beantragende Person wohnt, fungiert als *Sponsor* für Personen in dieser Gruppe und übernimmt die Aufgaben eines *Sponsors*.

e. Personenüberprüfungen: Personenüberprüfungen sind für Personen in dieser Gruppe nicht erforderlich.

f. Aufenthalts- und Arbeitserlaubnis: Personen in dieser Gruppe benötigen keine Aufenthalts- oder Arbeitserlaubnisse.

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen Zugang gewährt wird: Der Zugang ist auf das *BSB* zu beschränken, das als *Sponsor* fungiert. Die Zugangsberechtigung kann von diesem *BSB* weiter eingeschränkt werden. Personen, die im Besitz eines gültigen Besucherausweises sind und vorübergehend Zugang zu zusätzlichen Einrichtungen als den auf ihrem Ausweis angegebenen benötigen, kann in Begleitung der den Zugang beantragenden Person dieser erweiterte Zugang gewährt werden.

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Keine, es sei denn die beantragende Person oder der *Sponsor* verfügen welche.

i. Beschränkungen bzgl. der Eintragung von Personen in Besucherlisten: Personen dieser Gruppe ist diese Berechtigung nicht zu gewähren.

j. Sicherheitsstufenbezogene Beschränkungen: Eine Zugangsberechtigung unter Vorlage des Kasernenausweises besteht nur bei Sicherheitsstufe Alpha und Bravo. Eine einstufige Erweiterung der Zugangsberechtigung kann auf Antrag der *Sponsoring Organization* durch das *IACO* gewährt werden.

24. BESUCHER (FREUNDE, BEKANNTE ODER FAMILIENANGEHÖRIGE, DIE NICHT UNTER VORSTEHENDE PERSONENGRUPPE FALLEN)

a. Definition: Hierzu zählen alle Familienangehörigen, Freunde und Bekannte der beantragenden Person (Glossar), die 10 Jahre und älter sind und nicht unter vorstehende Gruppe (Abs. 23) fallen. Die Antragsteller haben den Nachweis zu erbringen, daß sie bei der beantragenden Person wohnen und ihr Abreisedatum feststeht. Diese Gruppe ist nicht heranzuziehen, um für am Wohnsitz der beantragenden Person lebenden Freunden oder Personen, die keine direkten Familienangehörigen sind, unbegleitet Zugang zu Einrichtungen der US-Streitkräfte zu verschaffen.

b. Folgende Ausweise können ausgestellt werden:

(1) Befristeter Kasernenausweis: Dieser Ausweis kann ausgestellt werden.

(2) Kasernenausweis: Personen in dieser Gruppe kann dieser Ausweis nur ausgestellt werden, wenn es sich um Familienangehörige handelt.

c. Gültigkeitsdauer der Ausweise: Die Gültigkeitsdauer des befristeten Kasernenausweises ist auf die Dauer des Besuchs bzw. auf bis zu 90 Tage begrenzt. Maßgebend ist der kürzere Zeitraum. Die Gültigkeitsdauer des Kasernenausweises ist auf die Dauer des Besuchs (mehr als 90 Tage) oder auf bis zu 1 Jahr bzw. bis zum Ablauf der Gültigkeit des für die Ausstellung vorgelegten Dokuments (z.B. Reisepass) begrenzt. Maßgebend ist der kürzere Zeitraum.

d. Erfordernisse bzgl. eines Sponsors: Das *BSB*, in dem die beantragende Person wohnt, fungiert als *Sponsor* für Personen in dieser Gruppe und übernimmt die Aufgaben eines *Sponsors*.

e. Personenüberprüfungen: Personenüberprüfungen sind für Personen in dieser Gruppe nicht erforderlich.

f. Aufenthalts- und Arbeitserlaubnis: Personen in dieser Gruppe benötigen keine Aufenthalts- oder Arbeitserlaubnisse.

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen Zugang gewährt wird: Die Ausweise sind auf das BSB, das als *Sponsor* fungiert, zu beschränken. Die Zugangsberechtigung kann von diesem BSB weiter eingeschränkt werden. Die Zugangsberechtigung kann nur auf die ASG ausgedehnt werden, wenn diese bereit ist, die Aufgaben der *Sponsoring Organization* wahrzunehmen. Personen, die im Besitz eines gültigen Besucherausweises sind und vorübergehend Zugang zu zusätzlichen Einrichtungen als den auf ihrem Ausweis angegebenen benötigen, kann in Begleitung der den Zugang beantragenden Person dieser erweiterte Zugang gewährt werden.

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Keine, es sei denn die beantragende Person oder der *Sponsor* verfügt über Beschränkungen.

i. Beschränkungen bzgl. der Eintragung von Personen in Besucherlisten: Personen dieser Gruppe ist diese Berechtigung nicht zu gewähren.

j. Sicherheitsstufenbezogene Beschränkungen: Eine Zugangsberechtigung unter Vorlage eines Kasernenausweises besteht nur bei Sicherheitsstufe Alpha und Bravo. Eine einstufige Erweiterung der Zugangsberechtigung kann auf Antrag der *Sponsoring Organization* durch das IACO gewährt werden.

25. OFFIZIELLE GÄSTE

a. Definition: Unter diese weitgefaßte Gruppe fallen alle Personen, die für dienstliche Zwecke, aufgrund einer dienstlichen Beziehung oder aufgrund eines mit der US-Regierung geschlossenen Abkommens zur gemeinschaftlichen Nutzung wiederholt Zugang benötigen (wie z. B. offizielle Vertreter von US-Bundesbehörden, Mitglieder in Vereinen oder Clubs, die ihren Sitz in einer US-Einrichtung haben (z. B. Schützen-, Tanzverein, Glider Club) oder Personen, die „in loco parentis“ Aufgaben wahrnehmen können und erziehungsberechtigt sind. Erfüllt ein Antragsteller die Kriterien einer anderen, restriktiveren Gruppe, so ist die Gruppe der „Offiziellen Gäste“ von der *Sponsoring Organization* bei Antragstellung nicht heranzuziehen.

ANMERKUNG: Personen, die „in loco parentis“ handeln, und andere im Haushalt lebende Personen, die Zugang zu Einrichtungen benötigen, haben eine Kopie des entsprechenden offiziellen Schreibens der *Host Nation Customs Policy Branch, Office of the Provost Marshal, HQ USAREUR/7A* bzw. von Formblatt *AE Form 600-700A* vorzulegen.

b. Folgende Ausweise können ausgestellt werden:

(1) **Befristeter Kasernenausweis:** Dieser Ausweis kann ausgestellt werden.

(2) **Kasernenausweis:** Dieser Ausweis kann ausgestellt werden.

c. Gültigkeitsdauer der Ausweise: Die Gültigkeitsdauer des befristeten Kasernenausweises ist auf 90 Tage begrenzt. Die Gültigkeitsdauer des Kasernenausweises ist auf bis zu 2 Jahre begrenzt bzw. bis zum Ablauf der Gültigkeit des für die Ausstellung vorgelegten Dokuments (z.B. Reisepass), der Gültigkeit des Abkommens zur gemeinschaftlichen Nutzung, des vorgelegten Schreibens oder der Mitgliedschaft. Maßgebend ist der kürzere Zeitraum.

d. Erfordernisse bzgl. eines Sponsors: Welche Organisation die Aufgaben der *Sponsoring Organization* übernimmt, hängt von der Funktion des offiziellen Gastes ab. In den meisten Fällen fungiert die ASG oder das BSB als *Sponsor* für Personen in dieser Gruppe und übernimmt die Aufgaben des *Sponsors*.

e. Personenüberprüfungen: Das ASG bzw. BSB, das die Aufgaben der *Sponsoring Organization* übernimmt, hat über die Notwendigkeit einer Personenüberprüfung zu entscheiden.

f. Aufenthalts- und Arbeitserlaubnis: Personen in dieser Gruppe benötigen keine Aufenthalts- oder Arbeitserlaubnisse.

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen Zugang gewährt wird: Die Anzahl der Einrichtungen ist auf das erforderliche Minimum zu beschränken.

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Die Tage/Zeiten, zu denen Zugang gewährt wird, sind von der *Sponsoring Organization* zu bestimmen.

i. Beschränkungen bzgl. der Eintragung von Personen in Besucherlisten: Personen dieser Gruppe ist diese Berechtigung nicht zu gewähren, es sei denn, es liegt eine Begründung von der *Sponsoring Organization* vor. Falls eine Berechtigung gewährt wird, können maximal 4 Personen mit ihren Fahrzeugen und diese auch nur für dienstliche Zwecke eingetragen werden.

j. Sicherheitsstufenbezogene Beschränkungen: Eine Zugangsberechtigung unter Vorlage eines Kasernenausweises besteht nur bis Sicherheitsstufe Charlie. Eine einstufige Erweiterung der Zugangsberechtigung kann jedoch auf Antrag der *Sponsoring Organization* durch das *IACO* gewährt werden.

26. MITARBEITER DES US-AUßENMINISTERIUMS UND DER US-BOTSCHAFT

a. Definition: Hierzu zählen alle Personen, die nach *USAREUR*-Dienstvorschrift 600-700 dem US-Außenministerium, einer im *USEUCOM AOR* gelegenen US-Botschaft, oder einer amerikanischen diplomatischen oder konsularischen Vertretung unterstellt sind.

b. Folgende Ausweise können ausgestellt werden:

(1) **Befristeter Kasernenausweis:** Dieser Ausweis kann nicht ausgestellt werden.

(2) **Kasernenausweis:** Dieser Ausweis kann ausgestellt werden.

c. Gültigkeitsdauer des Ausweises: Die Gültigkeitsdauer des Kasernenausweises ist bis zum Ende der Dienstzeit begrenzt (nicht länger als 5 Jahre) oder bis zum Ablauf der Gültigkeit des für die Ausstellung vorgelegten Dokuments (z.B. Reisepass, Formblatt *AE Form 600-700A*). Maßgebend ist der kürzere Zeitraum.

d. Erfordernisse bzgl. eines Sponsors: Die *U.S. Mission, Germany (U.S. Department of State)* fungiert als Sponsor für Personen in dieser Gruppe. Die bestellten *Sponsoring Officials* sind dem *USAREUR PM* von der *U.S. Mission, Germany*, per E-Mail mitzuteilen (*iacs@manupo.pmo.army.mil*). Der *PM* hat die Liste auf dem mit einer Zugangsbeschränkung versehenen Teil der *IACS*-Webseite zu veröffentlichen, wo sie allen *IACOs* von *USAREUR* zugänglich ist. Personen, die dieser Gruppe zuzurechnen sind, können sich in jedem *IACO* einen Kasernenausweis ausstellen lassen. Da diese Personen in ganz Deutschland verteilt sind, ist der erste Besuch einer von den US-Streitkräften kontrollierten Einrichtung mit der *Sponsoring Organization* und dem *IACO* zur Ausstellung eines Kasernenausweises gemäß Abs. 30b abzustimmen.

e. Personenüberprüfungen: Personenüberprüfungen sind für Personen in dieser Gruppe nicht erforderlich.

f. Aufenthalts- und Arbeitserlaubnis: Personen in dieser Gruppe benötigen keine Aufenthalts- oder Arbeitsgenehmigungen.

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen Zugang gewährt wird: Keine. Mitarbeiter des US-Außenministeriums und der US-Botschaft haben automatisch Zugang zu allen Einrichtungen der US-Streitkräfte. Eine Begründung ist hierfür nicht erforderlich.

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Es gibt keine Beschränkungen darüber, wann Zugang gewährt werden kann.

i. Beschränkungen bzgl. der Eintragung von Personen in Besucherlisten: Personen in dieser Gruppe können nur vier Personen mit Fahrzeugen in Besucherlisten eintragen.

j. Sicherheitsstufenbezogene Beschränkungen: Bezüglich der Sicherheitsstufen gelten keine Beschränkungen.

27. SONSTIGE

a. Definition: Hierzu zählen alle Personen, die wiederholt und ohne Begleitung Zugang benötigen, aber keiner der vorstehenden Gruppen in Abs. 12 bis 26, 28 oder 29 zuzurechnen sind. Diese Gruppe ist von den *Sponsoring Organizations* nicht zu wählen, wenn ein Antragsteller die Kriterien für die Zugehörigkeit zu einer der anderen, restriktiveren Gruppen erfüllt. Ein Beispiel für diese Kategorie sind Personen, die Beschäftigte der US-Streitkräfte täglich zum Dienst fahren und wieder abholen.

b. Folgende Ausweise können ausgestellt werden:

(1) Befristeter Kasernenausweis: Dieser Ausweis kann ausgestellt werden.

(2) Kasernenausweis: Dieser Ausweis kann ausgestellt werden.

c. Gültigkeitsdauer der Ausweise: Die Gültigkeitsdauer eines befristeten Kasernenausweises ist auf 90 Tage begrenzt. Die Gültigkeitsdauer eines Kasernenausweises ist auf 1 Jahr begrenzt oder bis zum Ablauf der Gültigkeit des für die Ausstellung vorgelegten Dokuments (z.B. Reisepass). Maßgebend ist der kürzere Zeitraum.

d. Erfordernisse bzgl. eines Sponsors: Das *BSB*, in dem Zugang benötigt wird, übernimmt die Funktion des *Sponsors* für diese Personen.

e. Personenüberprüfungen: Das *BSB*, das als *Sponsor* fungiert, entscheidet, ob Personenüberprüfungen erforderlich sind.

f. Aufenthalts- und Arbeitserlaubnis: Personen in dieser Gruppe benötigen keine Aufenthalts- oder Arbeitserlaubnisse.

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen Zugang gewährt wird: Der Zugang ist auf das *BSB*, das als *Sponsor* fungiert, zu beschränken. Die Zugangsberechtigung kann von diesem *BSB* weiter eingeschränkt werden. Die Zugangsberechtigung kann nur auf die *ASG* ausgedehnt werden, wenn diese bereit ist, die Aufgaben der *Sponsoring Organization* wahrzunehmen.

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Das als *Sponsor* fungierende *BSB* bestimmt über diesbezügliche Beschränkungen.

i. Beschränkungen bzgl. der Eintragung von Personen in Besucherlisten: Personen dieser Gruppe ist diese Berechtigung nicht zu gewähren.

j. Sicherheitsstufenbezogene Beschränkungen: Eine Zugangsberechtigung unter Vorlage eines Kasernenausweises besteht nur bei Sicherheitsstufe Alpha und Bravo. Eine einstufige Erweiterung der Zugangsberechtigung kann auf Antrag der *Sponsoring Organization* durch das *IACO* gewährt werden.

28. VERTRETER VON REGIERUNGSSTELLEN/BEHÖRDEN DES AUFNAHMESTAATES

a. Definition: Hierzu zählen alle Vertreter von Regierungsstellen/Behörden des Aufnahmestaates, die für dienstliche Zwecke bzw. aufgrund einer dienstlichen Beziehung wiederholt Zugang benötigen. Unter diese Gruppe fallen auch Vertreter der Stadt und Gemeinden (wie z. B. Bürgermeister/Bürgermeisterin, Feuerwehrkommandant und Mitarbeiter des örtlichen Bauamts), die US-Einrichtungen besuchen.

b. Folgende Ausweise können ausgestellt werden:

(1) Befristeter Kasernenausweis: Dieser Ausweis kann nicht ausgestellt werden.

(2) Kasernenausweis: Dieser Ausweis kann ausgestellt werden.

c. Gültigkeitsdauer des Ausweises: Die Gültigkeitsdauer des Kasernenausweises ist auf 5 Jahre beschränkt bzw. auf die Gültigkeit des für die Ausstellung vorgelegten Dokuments (z.B. Reisepass). Maßgebend ist der kürzere Zeitraum.

d. Erfordernisse bzgl. eines Sponsors: Welche Organisation die Aufgaben eines *Sponsors* wahrnimmt, hängt von der Funktion des Besuchers ab. Meist wird das *ASG* bzw. *BSB* als *Sponsor* für diese Personen fungieren und die entsprechenden Aufgaben wahrnehmen.

e. Personenüberprüfungen: Personenüberprüfungen sind für Personen dieser Gruppe nicht erforderlich.

ANMERKUNG: Vom Aufnahmestaat verpflichtete Personen und Firmen sind wie Mitarbeiter verpflichteter Privatfirmen (im Aufnahmestaat lebend) gemäß den Vorgaben in Abs. 15(e) zu überprüfen.

f. Aufenthalts- und Arbeitserlaubnis: Personen in dieser Gruppe benötigen keine Aufenthalts- oder Arbeitserlaubnisse.

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen Zugang gewährt wird: Die Zahl der Einrichtungen, zu denen Zugang gewährt wird, ist auf das zur Durchführung der Dienstgeschäfte erforderliche Minimum zu beschränken.

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Die Tage/Zeiten an/zu denen Zugang gewährt wird, sind von der Organisation, die die Aufgaben eines *Sponsors* wahrnimmt, zu bestimmen.

i. Beschränkungen bzgl. der Eintragung von Personen in Besucherlisten: Personen in dieser Gruppe wird keine Berechtigung zum Eintragen von Personen in Besucherlisten gewährt, es sei denn es liegt eine entsprechende Begründung der *Sponsoring Organization* vor. Falls aufgrund dieser Begründung eine Berechtigung gewährt wird, können maximal vier Personen mit ihren Fahrzeugen eingetragen werden und dies auch nur für dienstliche Zwecke.

j. Sicherheitsstufenbezogene Beschränkungen: Eine Zugangsberechtigung unter Vorlage des Kasernenausweises besteht nur bis Sicherheitsstufe Charlie. Eine Erweiterung der Zugangsberechtigung auf die nächste Sicherheitsstufe kann auf Antrag der *Sponsoring Organization* gewährt werden.

29. WACHPOSTEN

a. Definition: Wachposten kontrollieren den Zugang zu Einrichtungen. In der Regel handelt es sich hierbei um Mitarbeiter verpflichteter privater Wachfirmen. Sie führen ihre Aufgaben direkt am *ACP* durch und benötigen im Normalfall keinen Zugang zur Einrichtung selbst. Dieser Gruppe wird ausschließlich „logischer“ Zugang gewährt. Wachposten, die zur Wahrnehmung ihrer Aufgaben „physischen“ Zugang benötigen und denen eine entsprechende Berechtigung gewährt wird, wird als Mitarbeiter verpflichteter Privatfirmen (im Aufnahmestaat lebend) ein Kasernenausweis ausgestellt.

b. Folgende Ausweise können ausgestellt werden:

(1) **Befristeter Kasernenausweis:** Dieser Ausweis kann nicht ausgestellt werden.

(2) **Kasernenausweis:** Dieser Ausweis kann ausgestellt werden.

c. Gültigkeitsdauer des Ausweises: Die Gültigkeitsdauer des Kasernenausweises ist auf 2 Jahre beschränkt bzw. auf die Gültigkeit des für die Ausstellung vorgelegten Dokuments (z.B. Reisepass). Maßgebend ist der kürzere Zeitraum.

d. Erfordernisse bzgl. eines *Sponsors*: Der *Contracting Officer Representative (COR)* bzw. der *ASG Site Contracting Officer Representative (SCOR)* hat die Aufgaben eines *Sponsors* wahrzunehmen.

e. Personenüberprüfungen: Es ist davon auszugehen, dass Personenüberprüfungen vom *COR* bzw. *SCOR* als Voraussetzung für die Beschäftigung nach den Vorgaben von *AR 190-56* und *AE Regulation 190-13*, Kap. 7 abgeschlossen und überprüft wurden und über sie entschieden wurde. Zusätzliche Überprüfungen sind hier nicht erforderlich.

f. Aufenthalts- und Arbeitserlaubnis: Es ist davon auszugehen, dass eine entsprechende Aufenthalts- bzw. Arbeitserlaubnis durch den *COR* bzw. *SCOR* als Voraussetzung für die Beschäftigung überprüft wurde.

g. Beschränkungen bzgl. der Zahl der Einrichtungen, zu denen Zugang gewährt wird: Es wird nur „logischer“ Zugang gewährt.

h. Beschränkungen bzgl. der Tage/Zeiten, an/zu denen Zugang gewährt wird: Es wird nur „logischer“ Zugang gewährt.

i. Beschränkungen bzgl. der Eintragung von Personen in Besucherlisten: Personen in dieser Gruppe wird keine Berechtigung zum Eintragen von Personen in Besucherlisten gewährt.

j. Sicherheitsstufenbezogene Beschränkungen: Beschränkungen bestehen hier keine.

TEIL IV KASERNAUSWEIS

30. ANTRAGSVERFAHREN

a. *Sponsoring Officials* unterstützen berechtigte Personen bei der Beantragung eines Kasernenausweises beim zuständigen *IACO* durch Ausfüllen des Formblatts *AE Form 190-16A* (Anhang C). Formblatt *AE Form 190-16A* muss ausgefüllt werden, um

- (1) erstmals eine Kasernenausweis zu erhalten (Erstausstellung)
- (2) einen abgelaufenen oder in Kürze ablaufenden Ausweis zu erneuern (Abs. 32)
- (3) einen verloren gegangenen oder gestohlenen Ausweis zu ersetzen (Abs. 33)
- (4) einen befristeten Kasernenausweis zu verlängern (Abs. 34)
- (5) einen unbrauchbaren Ausweis zu ersetzen (Abs. 35).

ANMERKUNG: Antragsformulare sind auf Englisch, unter Angabe der üblichen amerikanischen Maßeinheiten, auszufüllen. Anhang D enthält eine Umrechnungstabelle für Körpergröße und Körpergewicht.

b. Wichtige Begriffe des Antragsschreibens:

(1) Sponsoring Organization: Die *Sponsoring Organization* hat innerhalb ihrer Organisation Personen zu bestimmen, die die Aufgaben der *Sponsoring Organization* erledigen. Welche Organisation als *Sponsoring Organization* für einen Antragsteller fungiert, hängt davon ab, welcher Gruppe der Antragsteller angehört (Abs. 12 bis 29). In manchen Fällen nimmt beispielsweise das *BSB* die Aufgaben einer *Sponsoring Organization* wahr, während in anderen Fällen diese Aufgabe der zukünftigen Beschäftigungsdienststelle des Antragstellers zukommt.

(2) Sponsoring Official:

(a) Der *Sponsoring Official* nimmt eine Schlüsselfunktion bei der Gewährleistung der Integrität des Programms zur Kontrolle der Zugangsberechtigung ein.

(b) Der Kommandeur bzw. der im Unterstellungsverhältnis erste *Lieutenant Colonel* oder *GS-13* einer Organisation, die für Personen, die einen Kasernenausweis beantragen, verantwortlich sind, haben schriftlich *Sponsoring Officials* zu benennen, die in Vertretung ihrer Organisation deren Aufgaben wahrnehmen. In *Sponsoring Organizations*, die diese Rang- bzw. Eingruppierungsstruktur nicht aufweisen (z.B. militärische Bankinstitute, regierungseigene Reisebüros), sind der 1. Geschäftsführer bzw. dessen Stellvertreter berechtigt, das Schreiben zur Benennung der *Sponsoring Officials* zu unterzeichnen. Diese Organisationen haben sicherzustellen, daß die beantragte Zugangsberechtigung auf das jeweilige *BSB* begrenzt ist. Außerdem haben diese *Sponsoring Organizations* sicherzustellen, daß der Sicherheitsmanager ihrer Organisation dem zuständigen *IACO* die Liste mit den Namen aller benannten *Sponsoring Officials* übermittelt (Anhang B). Das *IACO* hat dann

1. diese Liste abzulegen und auf dem neuesten Stand zu halten;

2. die Liste immer, wenn ein Antrag auf Ausstellung eines Kasernenausweises von dieser Organisation gestellt wird, zur Überprüfung der Autorisierung des *Sponsoring Official* und der korrekten Angabe der betreffenden Organisation als *Sponsoring Organization* heranzuziehen.

(c) *Sponsoring Officials* haben im Besitz einer *DOD ID-Card* oder ein vollzeitbeschäftigter ortsansässiger Arbeitnehmer zu sein. Nachstehende Tabelle zeigt, in welchem Umfang ein *Sponsoring Official* aufgrund seines Rangs bzw. seiner Eingruppierung Zugang für eine Person beantragen und befürworten kann.

1. Vorgesetzte im Rang eines *Sergeant-First-Class* (Oberfeldwebel) oder eines *Chief Warrant Officer 2* (Fachoffizier) sowie Zivilbedienstete, die als *GS-9* (US) oder *C-6A* (ortsansässige Arbeitnehmer) eingruppiert sind, können Zugang nur zu einer Einrichtung beantragen und befürworten.

2. Vorgesetzte im Rang eines *First Sergeant* (Kompaniefeldwebel) oder *Master Sergeant* (Stabsfeldwebel), *Chief Warrant Officer 3*, *Captain* (Hauptmann) sowie Zivilbedienstete, die als *GS-11* (US), *NF 4* oder *C-7* (ortsansässige Arbeitnehmer) eingruppiert sind, können *BSB*-weiten Zugang beantragen und befürworten.

3. Vorgesetzte im Rang eines *Sergeant Major* (Hauptfeldwebel), *Major* (Major), *Chief Warrant Officer 4* sowie Zivilbedienstete, die als *GS-12* (US), *NF 4* oder *C-7A* (ortsansässige Arbeitnehmer) eingruppiert sind, können *ASG*-weiten Zugang beantragen und befürworten.

4. Vorgesetzte im Rang eines *Lieutenant Colonel* (Oberstleutnant) sowie Zivilbedienstete, die als GS-13 (US), NF 5 oder C-8 (ortsansässige Arbeitnehmer) eingruppiert sind, können US-Streitkräfte-weiten Zugang beantragen und befürworten. Zusätzliche Beschränkungen für Antragsteller aus der Gruppe der im Aufnahmestaat lebenden Mitarbeiter verpflichteter Privatfirmen befinden sich in Abs. 15d.

ANMERKUNG: Die 22d und 80th ASG können für ihre ortsansässigen Arbeitnehmer die entsprechenden Eingruppierungsstufen zugrunde legen.

(d) NATO-Entsendestaaten und die *United States Mission, Germany*, haben die Liste ihrer bestellten *Sponsoring Officials* an den *USAREUR PM* zu senden. Der *PM* hat die Liste auf dem mit einer Zugangsbeschränkung versehenen Teil der *IACS*-Webseite zu veröffentlichen, wo sie allen *IACOs* von *USAREUR* zugänglich ist. *IACOs* haben ungeachtet der Vorgaben in vorstehenden Buchstaben (b) und (c) die auf der *IACS*-Webseite veröffentlichten Listen anzuerkennen.

(e) Die *Sponsoring Officials* haben die Einhaltung der in dieser Dienstvorschrift vorgegebenen Bestimmungen und Zielsetzungen sicherzustellen.

(3) Gruppen: Von der Personengruppe des Antragstellers hängt es ab, welcher Ausweis ausgestellt werden kann und welche Einschränkungen damit verbunden sind. Die Personengruppe des Antragstellers ist vom *Sponsoring Official* auf dem Antragschreiben (Feld 7) anzugeben. *IACO*-Registatoren haben die Richtigkeit der Angabe zu überprüfen. Welche Voraussetzungen für die Ausstellung eines Ausweises erfüllt sein müssen und welche Beschränkungen verfügt werden, sind je nach Zugehörigkeit des Antragstellers zu einer Personengruppe verschieden.

(4) Beantragter Ausweis: Je nach Personengruppe, welcher der Antragsteller angehört, und den Umständen, unter denen ein Antrag gestellt wird, kann ein befristeter Kasernenausweis oder ein regulärer Kasernenausweis beantragt werden.

(5) Personenüberprüfungen:

(a) Personenüberprüfungen werden durchgeführt, um festzustellen, ob der Antragsteller ein Sicherheitsrisiko darstellt. Welche Personenüberprüfung erforderlich ist, hängt von der Personengruppe der Antragsteller ab. Die *Sponsoring Organization* ist für die Durchführung der erforderlichen Personenüberprüfung verantwortlich. *IACO*-Registatoren haben zu prüfen, ob eine Personenüberprüfung durchgeführt wurde bzw. gegebenenfalls in die Weg geleitet wurde. Die *Sponsoring Organization* hat zur Bestimmung der erforderlichen Personenüberprüfung die jeweilige Personengruppe (Abs. 12 bis 29) anzugeben, der der Antragsteller zuzurechnen ist.

(b) Führt die Personenüberprüfung zu keinem nachteiligen Ergebnis, ist der Abschlussbericht an die *Sponsoring Organization* weiterzuleiten. Liegen nachteilige Informationen vor, ist der Bericht außerdem an die ASG, in dem der Antragsteller tätig wird, weiterzuleiten, damit diese in Abstimmung mit der *Sponsoring Organization* entscheiden kann, ob diese Informationen das Versagen einer Zugangsberechtigung rechtfertigen. Wenn der beantragte Zugang mehr als eine ASG umfasst, muss auch der *USAREUR PM* zu Rate gezogen werden. Bei der Entscheidung, ob nachteilige Informationen zu einem Versagen einer Zugangsberechtigung führen sollten, ist zu berücksichtigen, wie schwerwiegend die Informationen sind, und wie lange der Vorfall oder Verstoß, der zu den nachteiligen Informationen führte, zurückliegt.

(c) Im Folgenden werden die unterschiedlichen Personenüberprüfungen erläutert:

1. Polizeiliches Führungszeugnis: Der Antragsteller erhält dieses Zeugnis bei seinem zuständigen Ordnungsamt. Es wird auf der Grundlage von den deutschen Behörden zur Verfügung stehender Unterlagen erstellt und sollte am unteren Rand den Stempelvermerk: „Keine Eintragung“ aufweisen. Andere Vermerke sind zu übersetzen. Das Polizeiliche Führungszeugnis darf nicht älter als 12 Monate sein. Personen, die aufgrund der Zugehörigkeit zu einer bestimmten Personengruppe ein polizeiliches Führungszeugnis vorzulegen hätten, denen aber ein solches Zeugnis nicht ausgestellt werden kann (weil sie noch kein Jahr in Deutschland leben), haben ein entsprechendes Zeugnis ihres bisherigen Wohnsitzlandes mit englischer Übersetzung vorzulegen;

ANMERKUNG: Einigen nicht-deutschen Mitarbeitern verpflichteter Privatfirmen, die als technische Sachverständige tätig sind und denen ein Kasernenausweis ausgestellt werden muss, kann möglicherweise kein polizeiliches Führungszeugnis ausgestellt werden, weil sie nicht ihren gewöhnlichen Aufenthalt in Deutschland begründet haben. In diesem Fall sind vom *USAREUR PM* weitere Weisungen einzuholen.

2. Überprüfung durch die US-Militärpolizei: *Sponsoring Officials* können bei der zuständigen Militärpolizeidienststelle nachprüfen lassen, ob der Antragsteller aktenkundig ist. (**ANMERKUNG:** Dies gilt nur für US-Bürger.)

3. DCII: *DCII* ist das zentrale computergestützte Register der Ergebnisse aller von Ermittlungsbehörden des US-Verteidigungsministeriums durchgeführten Untersuchungen sowie aller von den entsprechenden Instanzen des US-Verteidigungsministeriums durchgeführten Personenüberprüfungen. In der *DCII*-Datenbank sind alle Sachtitel und Personen erfaßt, die in Ermittlungsunterlagen von Strafverfolgungsstellen des US-Verteidigungsministeriums, denen des Abschirmdienstes, Stellen zur Betrugsbekämpfung sowie Stellen zur Überprüfung von Personen als Gegenstand einer Untersuchung, in Zusammenhang mit einer Untersuchung, als Opfer oder als Personen, die zufällig in Zusammenhang mit einer Untersuchung (Zeugen) genannt wurden, erscheinen. Zu Ermittlungs-, gerichtlichen Feststellungs-, statistischen und Untersuchungszwecken sowie zu anderen genehmigten Zwecken werden Informationen von den Ermittlungsbehörden des US-Verteidigungsministeriums weitergegeben. Im *DCII* sind nur Personen erfaßt, denen eine *Social Security Number* ausgestellt wurde und die Verbindung zu den US-Streitkräften hatten. Die *Sponsoring Officials* können in Koordination mit dem Sicherheitsmanager ihrer Organisation den Standort des nächsten *DCII*-Zugriffendgeräts ermitteln. Bei Personen, die nach sicherheitsmäßiger Überprüfung als Geheimnisträger bereits Zugang zu geheimen und vertraulichen Informationen haben, ist eine *DCII*-Überprüfung nicht erforderlich.

4. FNS-Überprüfung: Mit Hilfe des Programms zur Überprüfung nicht-amerikanischer Staatsbürger wird vom *USAREUR PM* sichergestellt, daß nur zuverlässige ausländische Arbeitnehmer Zugang zu Einrichtungen erhalten. Eine *FNS*-Überprüfung kann auch für US-Bürger durchgeführt werden, die längere Zeit in Deutschland gelebt haben. *USAREUR G2* führt die Überprüfungen durch. Die *Sponsoring Organizations* haben die in *USAREUR Regulation 604-1* vorgegebenen Bestimmungen zur *FNS*-Überprüfung einzuhalten. Belege darüber, dass eine *FNS*-Überprüfung eingeleitet worden ist (in manchen Fällen vor Ausstellung eines befristeten Kasernenausweises erforderlich) bzw. abgeschlossen worden ist, sind auf der *FNS*-Webseite unter (<https://144.170.184.21/newweb/fnsp/>) erhältlich. Fragen über die *FNS*-Überprüfung sollten an die Einheit oder den zuständigen Sicherheitsbeauftragten der Organisation gerichtet werden.

ANMERKUNG: Formblatt *AE Form 604-1B* (abzurufen unter: <https://www.aeaim.hqusareur.army.mil/library/for/index-aeform604-1b.pdf>) ist von den Personen, für die eine *FNS*-Überprüfung durchgeführt wird, zu unterschreiben. Das unterschriebene Formblatt ist jedoch nicht dem Antragspaket beizulegen und beim zuständigen *IACO* abzugeben.

(d) Aufgrund des Herkunftslandes oder der Zeit, die der Antragsteller in Deutschland lebt, kann es sein, dass eine Personenüberprüfung für einen Antragsteller nicht in Frage kommt. Damit eine *FNS*-Überprüfung eingeleitet werden kann, muss der Antragsteller z. B. die letzten 12 Monate oder länger in Deutschland gelebt haben. Ein weiteres Beispiel betrifft Antragsteller in der Personengruppe Händler/Dienstleister, die aus anderen Ländern kommen, um ihre Waren zu verkaufen. Obwohl eine *BSB* die Vollmacht hat, die Ausstellung eines Kasernenausweises zu verweigern, weil sie die Personenüberprüfungen nicht durchführen kann und somit die Unbedenklichkeit des Antragstellers nicht prüfen kann, sollten die *BSBs* von Fall zu Fall entscheiden und die Entscheidung aufgrund des Risikos, das der Antragsteller darstellt, fällen. *BSBs* können das Risiko durch Anwendung einer oder mehrerer der folgenden Strategien reduzieren:

1. Wenn der Antragsteller keinen deutschen Wohnsitz hat, muss der Antragsteller aufgefordert werden, ein ins Englische übersetztes, beglaubigtes Dokument aus seinem Land vorzulegen, das dem polizeilichen Führungszeugnis entspricht;

2. Genauere Prüfung der Zugangsprivilegien und Beschränkung der Anzahl der Einrichtungen und Zeiten, zu denen Zugang erlaubt ist;

3. Wenn die Personengruppe befugt ist, Personen in Besucherlisten einzutragen, wird allen Personen, über die keine angemessenen Informationen aus Personenüberprüfungen vorliegen, diese Befugnis verweigert;

4. Die Gültigkeit von Kasernenausweisen ist so wählen, dass sie zu dem Datum abzulaufen, zu dem der Wohnsitz in Deutschland 1 Jahr besteht und somit eine *FNS*-Überprüfung durchgeführt werden kann.

(6) Aufenthalts- und Arbeitserlaubnis

(a) In der Regel können alle nicht-deutschen Staatsbürger für die US-Streitkräfte in Deutschland tätig werden, wenn sie im Besitz einer gültigen Aufenthaltserlaubnis/Aufenthaltsberechtigung/Aufenthaltsbewilligung sowie einer Arbeitserlaubnis sind.

(b) Personen, die einen Kasernenausweis beantragen, haben zur Ausstellung eine gültige Aufenthalts- und Arbeitserlaubnis vorzulegen, es sei denn, sie sind gemäß d unten von der Vorlage dieser Dokumente befreit.

(c) Falls als Voraussetzung für die Registrierung für die betreffende Personengruppe angegeben, haben nicht-deutsche Staatsbürger sowie vom US-Verteidigungsministerium verpflichtete Mitarbeiter von Privatfirmen in Deutschland eine Kopie ihrer Aufenthalts- und Arbeitserlaubnis vorzulegen. Die Aufenthaltserlaubnis wird durch Stempelindruck im Reisepass erteilt, die Arbeitserlaubnis auf einem separaten Formblatt.

ANMERKUNG: Bei einem zusammenhängenden Aufenthalt von mehr als 90 Tagen ist eine Aufenthaltserlaubnis vorzulegen.

(d) Bürger aus EU-Staaten haben keine Arbeitserlaubnis vorzulegen; sie sollten aber eine EU-Aufenthaltserlaubnis besitzen (separates Formblatt), sofern sie ihren ständigen Wohnsitz in Deutschland haben. Folgende Personen sind außerdem von der Vorlage einer Arbeitserlaubnis befreit:

1. Soldaten, Angehörige des zivilen Gefolges, Bedienstete von US-Organisationen und Mitarbeiter verpflichteter Privatfirmen, die unter Artikel 71 - 73 des Zusatzabkommens zum NATO-Truppenstatut fallen;

2. Nicht-deutsche Staatsbürger, die in einem Verwandtschaftsverhältnis zu Angehörigen der US-Streitkräfte bzw. zu dem zivilen Gefolge unterstellten Mitarbeitern stehen;

3. An deutschen Universitäten Studierende, die aus Nicht-EU-Staaten kommen. Sie sind ebenfalls von der Vorlage einer Arbeitserlaubnis befreit, wenn sie weniger als 3 Monate während der Semesterferien beschäftigt werden. Sie haben allerdings eine Aufenthaltserlaubnis vorzulegen.

(7) Anzahl der Einrichtungen, zu denen Zugang gewährt werden soll

(a) Eine wesentliche Zielsetzung des Zugangskontrollprogramms ist die Beschränkung der Zugangsberechtigung auf die geringstmögliche Zahl von Einrichtungen.

(b) Folgenden Personengruppen wird ohne nähere Begründung Zugang zu allen Einrichtungen der US-Streitkräfte im *USAREUR AOR* gewährt:

1. Inhabern von *DOD ID-Cards* (Abs. 12)

2. NATO-Angehörigen (Abs. 19)

3. Mitarbeitern des US-Außenministeriums und der US-Botschaft (Abs. 26)

(c) Ist für eine Person der Zugang zu Einrichtungen im *USAREUR AOR* zu begründen, hat der *Sponsoring Official* dieser Person Folgendes zu beachten:

1. Er hat sicherzustellen, daß auf dem Antrag die Einrichtungen angegeben sind, zu denen mindestens Zugang gewährt werden soll. Dabei sind die Namen der jeweiligen *ASG*, *BSB* bzw. der Einrichtung(en) anzugeben (z.B. "Ausschließlich Taylor Barracks und Coleman Barracks" oder "Ausschließlich 293rd *BSB*"). Ist einem Antragsteller Zugang zu mehr als einem *BSB* oder einer Einrichtungen zu gewähren, so ist dies umfassend und stichhaltig zu begründen.

2. Wenn ein Antragsteller in Deutschland *USAREUR*-weiten Zugang benötigt, ist anzugeben, ob sich dies ausschließlich auf Einrichtungen der Armee oder auch auf Einrichtungen der US-Luftwaffe bezieht. Aus dem Antrag muss auch hervorgehen, ob Zugang zu der 22d *ASG* und der 80th *ASG* erforderlich ist. Ist Zugang zu Einrichtungen im Verantwortungsbereich der 22d *ASG* erforderlich, hat der Antrag eine schriftliche Genehmigung vom 22d *ASG PMO* zu enthalten.

(d) Hat für die Zugangsberechtigung zu Einrichtungen im *USAREUR AOR* eine Begründung vorzuliegen, haben die Ausweise ausstellenden Mitarbeiter im *IACO*

1. sicherzustellen, daß die *Sponsoring Officials* eine Zugangsberechtigung nur in dem Umfang beantragen, zu dem sie autorisiert sind;

2. nicht stichhaltige und unzureichende Begründungen in Abstimmung mit dem *Sponsoring Official* abzuklären;

3. alle Anträge für Personen der Gruppe „Mitarbeiter verpflichteter Privatfirmen (im Aufnahmestaat lebend)“ sorgfältig zu prüfen, um sicherzustellen, daß der beantragte Umfang der Zugangsberechtigung den Vorgaben in Abs. 15 entspricht.

(8) Tage/Zeiten, an/zu denen Zugang zu gewähren ist: Die *Sponsoring Officials* haben sicherzustellen, daß auf dem Antrag die Tage und Zeiten, an/zu denen mindestens Zugang zu gewähren ist, angegeben sind.

(9) Berechtigung zum Eintragen von Personen in Besucherlisten: Eine Berechtigung zum Eintragen von Personen in Besucherlisten ist nur dann zu beantragen, wenn dafür eine wirklicher Grund angegeben werden kann. Aus der Begründung hat hervorzugehen, daß die Berechtigung zum Eintragen von Personen für den Ausweisinhaber oder die *Sponsoring Organization* nicht nur bequem ist, sondern daß dafür eine echte Notwendigkeit besteht. Diese Notwendigkeit ist genauestens zu erläutern. In den meisten Fällen ist die Berechtigung auf andere Mitarbeiter verpflichteter Privatfirmen und Personen beschränkt, die für dienstliche Zwecke Zugang benötigen, und erstreckt sich nicht auf Personen, die für persönliche Zwecke Zugang möchten. Ausgenommen von Vorstehendem sind lediglich „NATO-Angehörige“ (Abs. 19) und „Mitarbeiter des US-Außenministeriums und der US-Botschaft“ (Abs. 26). Personen, die diesen Gruppen zuzurechnen sind, sind automatisch berechtigt, Personen in Besucherlisten einzutragen.

(a) Inhaber von Kasernenausweisen, die berechtigt sind, Personen in Besucherlisten einzutragen, haben die für die Eintragung vorgeschriebenen Verfahren in Abs. 41 einzuhalten.

(b) Wird für „Mitarbeiter verpflichteter Privatfirmen (im Aufnahmestaat lebend)“ eine Berechtigung zum Eintragen von Personen in Besucherlisten beantragt, haben die *IACO*-Registrierer sicherzustellen, daß der *Sponsoring Official*, der diese Berechtigung beantragt, die entsprechenden Voraussetzungen im Hinblick auf Rang bzw. Eingruppierung erfüllt (Abs. 15d).

(c) Inhaber befristeter Kasernenausweise erhalten keine Berechtigung zum Eintragen von Personen in Besucherlisten.

(d) Personen in Gruppen, in denen eine Berechtigung zum Eintragen von Personen in Besucherlisten möglich ist, dürfen nicht mehr als vier Personen mit ihren Fahrzeugen eintragen.

(10) Sicherheitsstufenbezogene Beschränkungen: Die Beschränkungen im Hinblick auf die Sicherheitsstufen richten sich nach der Gruppe, der die Person zuzuordnen ist. Das *IACS* gewährt nur bei den für die jeweilige Personengruppe gültigen Sicherheitsstufen Zugang (Abs. 12 bis 29). Sollten *Sponsoring Officials* die Zugangsberechtigung bei den Sicherheitsstufen weiter einschränken wollen, ist dies im Antrag genau anzugeben.

(11) Angaben zum Kraftfahrzeug: Alle Personen, die die Ausstellung eines Kasernenausweises beantragen, haben die Kraftfahrzeuge, mit denen sie in Einrichtungen der US-Streitkräfte im *USAREUR AOR* einfahren wollen, anzumelden. Die Erfordernis der Anmeldung und Zuordnung zu den *IACS*-Daten eines Antragstellers gilt nur für Privatfahrzeuge, nicht aber für Firmenfahrzeuge. Der Nachweis über das Eigentum an dem Fahrzeug ist für die Registrierung im *IACS* nicht zu führen und darf auch niemals als Grund zur Verweigerung eines regulären oder befristeten Kasernenausweises herangezogen werden. Folgende Angaben zum Fahrzeug sind auf dem Antrag (Formblatt *AE Form 190-16A*) in den Feldern 24 und 25 zu machen:

(a) Kennzeichen und Ausstellungsland

(b) Marke/Bauart/Baujahr/Karosserietyp und Farbe

(c) Name und Telefonnummer der Firma (Dies gilt nur für die Gruppe „Mitarbeiter verpflichteter Privatfirmen (im Aufnahmestaat lebend)“.)

c. Nach Abfassung des Antrags hat der *Sponsoring Official* den Antragsteller zu dem für ihn zuständigen *IACO* zu begleiten (d unten). Alle für die Ausstellung erforderlichen Dokumente sind mitzunehmen. Kann der *Sponsoring Official* den Antragsteller nicht begleiten und kann der Antragsteller nur auf diesem Wege eine Zugangsberechtigung für die Einrichtung erhalten, kann wie nachstehend ausgeführt vorgegangen werden.

(1) Der *Sponsoring Official* hat den Antrag auf Ausstellung eines Kasernenausweises per E-Mail an das zuständige *IACO* zu senden und dem für die Ausstellung zuständigen *IACO*-Mitarbeiter das ungefähre Datum und die ungefähre Uhrzeit, zu der der Antragsteller bei der Einrichtung eintrifft, mitzuteilen.

(2) Der für die Ausstellung zuständige *IACO*-Mitarbeiter hat anhand der von der *Sponsoring Organization* eingereichten Liste ihrer bestellten Vertreter sicherzustellen, daß der Absender der E-Mail berechtigt ist, die Aufgaben eines *Sponsoring Officials* wahrzunehmen.

(3) Bei Eintreffen des Antragstellers am *ACP* hat der Wachposten beim *IACO* anzurufen, um sich zu vergewissern, daß der Antragsteller erwartet wird und das *IACO* per E-Mail von der *Sponsoring Organization* benachrichtigt wurde.

(4) Der Wachposten hat den Reisepass bzw. Personalausweis (je nachdem, welches Dokument auf dem unterschriebenen Antrag, den der Antragsteller mit sich zu führen hat, angegeben ist) zu überprüfen und dem Antragsteller ohne Begleitung Zugang zu gewähren.

(5) Das unterschriebene Original des Antrags hat der Antragsteller dem *IACO* vorzulegen und sich einen Kasernenausweis ausstellen zu lassen.

ANMERKUNG: Antragsteller haben ähnlich vorzugehen, wenn sie Zugang zur Einrichtung erhalten, der *Sponsoring Official* sie aber nicht zu dem zuständigen *IACO* begleiten kann. Unter keinen Umständen ist einem Antragsteller vom *IACO* ein Kasernenausweis in Abwesenheit eines *Sponsoring Official* bzw. ohne vorherige Absprache mit dem *IACO* auszustellen.

d. Zusammen mit dem Antrag sind von den Antragstellern folgende Unterlagen vorzulegen:

(1) eine Kopie von einem der folgenden Dokumente:

(a) Reisepass

(b) Personalausweis des Landes, in dem die Staatsbürgerschaft besteht (z.B. deutscher, belgischer oder italienischer Personalausweis)

(c) von einem der NATO-Entsendestaaten (Belgien, Frankreich, Großbritannien, Kanada, Niederlande) ausgestellten Militärausweis;

(2) eine Kopie des Ergebnisberichts aller erforderlichen Personenüberprüfungen;

(3) der Nachweis, daß der Antragsteller im Besitz einer eventuell erforderlichen gültigen Aufenthalts- und Arbeitserlaubnis ist;

(4) eine Kopie der Mitgliedsurkunde; eines entsprechenden Schreibens, aus dem hervorgeht, dass sie „in loco parentis“ handeln; von Formblatt *AE Form 600-700A* bzw. des entsprechenden Vertrags als Begründung der Notwendigkeit des Zugangs. Außerdem ist die Gültigkeitsdauer zu belegen.

ANMERKUNG: Ein Foto hat der Antragsteller nicht mitzubringen.

31. ANTRAGSVERFAHREN FÜR INHABER EINES BEFRISTETEN KASERNENAUSWEISES

a. In diesem Fall ist von der *Sponsoring Organization* kein neuer Antrag zu stellen.

b. Die *Sponsoring Officials* haben dem *IACO* persönlich oder per E-Mail mitzuteilen, wo der befristete Kasernenausweis ausgestellt und wann die *FNS*-Überprüfung abgeschlossen wurde.

c. Erfolgt die Mitteilung per E-Mail, hat der für die Ausstellung zuständige *IACO*-Mitarbeiter anhand der von der *Sponsoring Organization* eingereichten Liste ihrer bestellten Vertreter (Anhang B) sicherzustellen, daß der Absender der E-Mail berechtigt ist, die Aufgaben eines *Sponsoring Officials* wahrzunehmen.

d. In der Mitteilung an das *IACO* ist das genaue Datum des Abschlusses der *FNS*-Überprüfung anzugeben. Außerdem ist zu bestätigen, daß laut Ergebnisbericht keine nachteiligen Informationen über den Antragsteller vorliegen. Sollten nachteilige Informationen vorliegen, so ist zu bestätigen, daß die *ASG*, für die der Antragsteller tätig wird, und der *Sponsoring Official* den Bericht überprüft haben und zu dem Ergebnis gekommen sind, daß die vorliegenden nachteiligen Informationen die Verweigerung einer Zugangsberechtigung nicht rechtfertigten. Darüber hinaus hat der *Sponsoring Official* in der Mitteilung alle Änderungen, die seit Ausstellung des befristeten Kasernenausweises eingetreten sind, anzugeben.

e. Nach Erhalt der Mitteilung hat der Antragsteller seinen befristeten Kasernenausweis abzugeben und sich einen regulären Kasernenausweis ausstellen zu lassen. Die Mitteilung wird zusammen mit den Originalunterlagen des Antrags auf Erstellung eines befristeten Kasernenausweises abgelegt.

32. ANTRAGSVERFAHREN ZUR ERNEUERUNG EINES KASERNENAUSWEISES

a. Zur Erneuerung eines abgelaufenen Kasernenausweises muss die *Sponsoring Organization* zur Bestätigung der auf dem Originalantrag gemachten Angaben einen neuen Antrag (Formblatt *AE Form 190-16A*) stellen.

b. Folgendes gilt für Personenüberprüfungen, wenn ein Antragsteller seinen Kasernenausweis erneuert:

(1) Ein neues polizeiliches Führungszeugnis muss vorgelegt werden, wenn die beiden folgenden Punkte zutreffen:

(a) Für die Gruppe der Person war ein polizeiliches Führungszeugnis erforderlich. Für die Gruppe „Ortsansässige Beschäftigte“ (Abs. 13) ist dies nicht erforderlich.

(b) Das letzte polizeiliche Führungszeugnis ist älter als 12 Monate.

(2) Eine erneute Überprüfung durch die Militärpolizei ist erforderlich, wenn eine solche Überprüfung aufgrund der Personengruppe, der der Antragsteller zuzurechnen ist, für die Erstaussstellung erforderlich war. (Personen, die der Gruppe der ortsansässigen Arbeitnehmer zuzurechnen sind (Abs. 13) und vor dem 3. Oktober 1985 eingestellt wurden, waren von dieser Regelung ausgenommen.)

(3) Eine erneute *DCII*-Überprüfung ist erforderlich, wenn aufgrund der Personengruppe, der der Antragsteller zuzurechnen ist, eine solche Überprüfung für die Erstaussstellung erforderlich war.

(4) Soweit keine außergewöhnlichen Umstände gegeben sind, ist eine erneute *FNS*-Überprüfung nicht erforderlich. Die *Sponsoring Officials* haben sich auf die Ergebnisse der ersten *FNS*-Überprüfung zu stützen.

c. Ablaufende oder abgelaufene Ausweise sind abzugeben, bevor neue ausgestellt werden können. Wurde der abgelaufene Ausweis von Wachposten eingezogen, ist als Einzugs-/Empfangsbestätigung Formblatt *AE Form 190-16B* vorzulegen.

ANMERKUNG: Ortsansässige Arbeitnehmer (Abs. 13), die ohne Dienstunterbrechung von einer Dienststelle der US-Streitkräfte in eine andere wechseln, behalten ihren Status bei. Ein neues polizeiliches Führungszeugnis ist deshalb nicht vorzulegen. Auch ist keine erneute Überprüfung durch die amerikanische Militärpolizei durchzuführen. Der Dienststellenwechsel ist auf dem neuen Antrag zu vermerken.

33. ANTRAGSVERFAHREN BEI ANTRAG AUF ERSATZ EINES GESTOHLLENEN BZW. VERLORENGEGANGENEN KASERNENAUSWEISES

Der Verlust bzw. Diebstahl eines Kasernenausweises ist umgehend der örtlichen Militärpolizeidienststelle und dem *IACO* zu melden, damit der Ausweis im *IACS* entsprechend gekennzeichnet werden kann. Zur Ausstellung eines neuen Ausweises ist von der *Sponsoring Organization* bei dem *IACO*, das den gestohlenen bzw. verlorengegangenen Ausweis ausstellte, ein neuer Antrag zu stellen. Falls vom *Sponsoring Official* im Antragschreiben beantragt, kann die Gültigkeitsdauer des neuen Ausweises verlängert und auf den für die Personengruppe zulässigen vollen Zeitraum ausgedehnt werden.

34. ANTRAGSVERFAHREN ZUR VERLÄNGERUNG EINES BEFRISTETEN KASERNENAUSWEISES

a. Befristete Kasernenausweise können nur einmalig aufgrund einer stichhaltigen Begründung um höchstens 90 Tage verlängert werden. Die Möglichkeit zur Gewährung einer einmaligen Verlängerung des Ausweises soll hauptsächlich dazu dienen, dem Ausweisinhaber weiterhin Zugang zu Einrichtungen zu gewähren, wenn es bei der Übermittlung der Ergebnisse der *FNS*-Überprüfung zu einer unvorhergesehenen Verzögerung kommt. Falls die *FNS*-Überprüfung abträgliche Ergebnisse aufzeigt, die die Ablehnung eines Kasernenausweises rechtfertigen, wird dem Inhaber eines befristeten Kasernenausweises kein weiterer befristeter Kasernenausweis mehr ausgestellt. Bei Überprüfungen, die zu abträglichen Ergebnissen führen, ist nach Abs. 5c(4), 5e(4), 5h(2), 5i(1) und 5k(3) vorzugehen.

b. Der *Sponsoring Official* hat die Verlängerung mit dem *IACO*, das den befristeten Kasernenausweis ausstellte, abzustimmen. Wird eine Verlängerung vom ausstellenden Mitarbeiter des *IACO* genehmigt, hat der Ausweisinhaber seinen befristeten Kasernenausweis beim zuständigen *IACO* abzugeben. Er erhält dann einen neuen befristeten Ausweis mit neuer Gültigkeitsdauer.

c. Sind nicht rechtzeitig vorliegende Ergebnisse der *FNS*-Überprüfung der Grund für einen Antrag auf Verlängerung, hat der für die Ausstellung des Ausweises zuständige *IACO*-Mitarbeiter in Zusammenarbeit mit dem zuständigen *S2* oder *Security Manager* den Stand der Überprüfung zu ermitteln.

d. Diese einmalige Verlängerung (s. vorstehenden Abs. a) ist nicht dazu zu nutzen, die strengeren Voraussetzungen für die Ausstellung eines regulären Kasernenausweises zu umgehen.

e. Befristete Kasernenausweise, die aufgrund ausstehender Ergebnisse der *FNS*-Überprüfung bereits 90 Tage verlängert wurden (Gesamtgültigkeit somit 180 Tage), können trotz weiterhin ausstehender *FNS*-Ergebnisse nur mit ausdrücklicher Genehmigung des *USAREUR PM* ein weiteres Mal verlängert werden.

35. UNBRAUCHBARE KASERNENAUSWEISE

Unbrauchbare Ausweise können bei dem für die Ausweisinhaber zuständigen *IACO* gegen neue eingetauscht werden, und zwar ohne irgendwelche Maßnahmen seitens der *Sponsoring Organization*. Der unbrauchbare Ausweis ist abzugeben, es sei denn er wurde von der Militärpolizei oder einem Wachposten eingezogen (Abs. 44a(4)). Wurde der unbrauchbare Ausweis von der Militärpolizei oder einem Wachposten eingezogen, ist Formblatt *AE Form 190-16B* als Einzugs-/Empfangsbestätigung auszustellen und zur Ausstellung eines neuen Ausweises vorzulegen (Abbildung 2). Die Gültigkeitsdauer des neuen Ausweises hat der des ursprünglich ausgestellten zu entsprechen.

RECEIPT FOR CONFISCATED ID CARD (AE Reg 190-16)	
Mr./Mrs./Miss <u>Joe M. Smith</u>	
This is a receipt for your ID card. The ID card must be turned in. It is invalid because it—	
<input checked="" type="checkbox"/> is mutilated	<input type="checkbox"/> is expired
<input type="checkbox"/> has been obviously altered	
It has no further use. It is Government property. Access-control personnel are authorized by AR 600-8-14 to confiscate invalid Government cards. Please contact the proper installation authority for card replacement. This ID card will be turned over to the local military law enforcement activity for disposition.	
Card number 123-45-6789	Date confiscated 1 January 2005
Signature (access-control personnel)	
Location and name of facility 293d BSB, Mannheim, Sullivan Barracks ACP	
AE FORM 190-16B, MAR 05 Previous editions are obsolete.	

Abbildung 2. Formblatt *AE Form 190-16B* (Muster)

TEIL V

INSTALLATION ACCESS CONTROL OFFICE (IACO)

36. ALLGEMEINES

a. Nur von *USAREUR* zugelassene *IACOs* sind zur Ausstellung von Kasernenausweisen berechtigt. Eine vollständige Liste aller zugelassenen *IACOs* kann unter <http://www.hqusareur.army.mil/opm/iacs/Resources/USAREURIACSRegistrationStations.pdf> abgerufen werden.

b. Mit Ausnahme einiger *Default Settings* im *IACS* gibt es nur wenige Einschränkungen, was die Arten von Ausweisen betrifft, die vom *IACO* ausgestellt werden können. Jedes *IACO* ist z.B. befugt, *USAREUR*-weit gültige Ausweise auszustellen. Diese Befugnis wird unter der Voraussetzung gewährt, daß die *IACOs* die in dieser Dienstvorschrift vorgegebenen Richtlinien, Verfahren und Zielsetzungen einhalten und der *USAREUR PM* die Nutzer-Aktivitäten im *IACS* überwacht.

c. Die Zugangskontrolle ist Aufgabe der Standortkommandeure. Organisationen außerhalb der direkten Kontrolle der ASGs bzw. BSBs sind nicht befugt, Ausweise auszustellen und werden deshalb auch nicht mit dem IACS ausgestattet.

d. IACOs werden vor der Einsatz- und Betriebsbereitschaft des IACS zugelassen. Anträge auf Zulassung weiterer IACOs oder IACS-Registrierungsstellen nach Einsatz- und Betriebsbereitschaft des IACS sind auf dem vorgeschriebenen Dienstweg an den USAREUR PM (AEAPM-O-SO), Unit 29931, APO AE 09086-9931 zu richten.

e. Die BSBs sollten ihre IACOs der zuständigen Militärpolizeidienststelle angliedern.

f. IACO-Registatoren haben

(1) alle Vorfälle, bei denen falsche Angaben gemacht werden oder versucht wird, das System zur Ausstellung von Ausweisen zu manipulieren, der Militärpolizei zu melden;

(2) unter Entwicklung eines entsprechenden Systems alle 6 Monate mit der *Sponsoring Organization* eine Abgleichung vorzunehmen, um sicherzustellen, daß die im IACS erfaßten Personen noch zugangsberechtigt sind;

(3) zur Gewährleistung der Sicherheit, der Nachweisführung und der Beschaffung von Ausweismaterial folgendermaßen vorzugehen:

(a) Bei der Aufbewahrung der weißen Blankoausweise sind keine speziellen Sicherheitsmaßnahmen und Nachweisverfahren zu befolgen.

(b) IACO-Registatoren haben über jede Vernichtung eines Ausweises Buch zu führen und diese auf Formblatt *AE Form 190-16C* zu dokumentieren und im IACS zu erfassen. Dieses Formblatt kann unter <https://www.aeaim.hqusareur.army.mil/library/for/index-aef.shtm> abgerufen werden.

(c) Blankoausweise, Folienmaterial und Drucker-Farbbänder werden den IACOs vom USAREUR PM zur Verfügung gestellt. IACOs haben stets einen angemessenen Vorrat an Blankoausweisen, Folienmaterial und Drucker-Farbbändern vorzuhalten.

37. REGISTRIERUNG VON PERSONEN, DIE EINEN KASERNENAUSWEIS BEANTRAGEN

a. IACO-Registatoren haben bei der Bearbeitung von Anträgen auf Ausstellung eines Kasernenausweises folgendermaßen vorzugehen:

(1) Kann der *Sponsoring Official* den Antragsteller nicht zum IACO begleiten, sind die in Abs. 30c vorgegebenen Verfahren einzuhalten, damit der Antragsteller zur Ausstellung des Ausweises Zugang zur Einrichtung hat.

(2) Anhand der von der *Sponsoring Organization* eingereichten und abgelegten Liste ihrer *Sponsoring Officials* ist zu überprüfen, ob der Antragsunterzeichner die entsprechende Autorisierung besitzt. Anträge, die von einer nicht dazu berechtigten Person unterschrieben sind, sind abzulehnen.

(3) Für die Ausweisausstellung sind der Antrag und die für die Ausstellung erforderlichen Dokumente vom Antragsteller entgegenzunehmen. Anträge, denen nicht alle erforderlichen Dokumente beigelegt sind, sind abzulehnen. Für die erfolgreiche Durchführung des *Installation Access Control Program* ist es unabdingbar, dass die Registatoren alle erforderlichen Unterlagen genauestens überprüfen. Nur so kann die Wahrscheinlichkeit, dass Personen, die ein großes Sicherheitsrisiko darstellen, Zugang zu Einrichtungen der US-Streitkräfte im USAREUR AOR haben, auf ein Mindestmaß reduziert werden.

(4) Der Antragsteller ist unter Eingabe der im Antrag gemachten Angaben im IACS zu registrieren. Werden Beschränkungen verfügt (z.B. im Hinblick auf die Berechtigung zum Eintragen von Personen in Besucherlisten oder die Zahl der Einrichtungen, zu denen Zugang gewährt werden soll), sind diese vom *Sponsoring Official* schriftlich zu begründen. Der Registrator hat nicht-stichhaltige und unzureichende Begründungen abzuklären und trägt damit zur Qualitätskontrolle des gesamten Systems bei. Besonders wenn USAREUR-weiter Zugang beantragt wird, haben die Registatoren zu prüfen, ob der Antragsteller lediglich eine niedrigere Zugangsstufe benötigt, wie z.B. USAREUR-weit (nur Deutschland).

(5) Vor Aushändigung des Ausweises hat der Antragsteller eine Anerkennung seiner Pflichten (Anhang E) und eine Erklärung zum US-Datenschutzgesetz (*U.S. Privacy Act*) (Abb. 3) unter Angabe des Datums zu unterzeichnen. Der Antragsteller erhält eine Kopie der Anerkennung seiner Pflichten zur Aufbewahrung. Die Erklärung zum US-Datenschutzgesetz (*U.S. Privacy Act*) ist nur für US-Staatsangehörige erforderlich.

PRIVACY ACT STATEMENT

AUTHORITY: Public Law 106-246, Title 10 USC, DODD 8500.1, AR 25-2, and EO 9397.

PRINCIPAL PURPOSE: To control local access to DOD information or information-based systems, and to control the physical access to installations, buildings, and controlled spaces by using measurable physical or behavioral characteristics to maintain accountability for issuance and disposition of installation passes.

ROUTINE USES: None. The "Blanket Routine Uses" are set forth at the beginning of the Army's compilation of systems of records notices.

DISCLOSURE: Voluntary. Failure to provide the requested information may result in denial of access to DOD information-based systems, DOD facilities, or both.

By signing below, I acknowledge that I have read and understand the conditions set forth in the above Privacy Act statement.

Printed Name

Signature

Date

Abbildung 3. Erklärung zum US-Datenschutzgesetz (U.S. Privacy Act)

Eine deutsche Version der Datenschutzerklärung/Privacy Act Statement mit englischer Übersetzung befindet sich am Ende.

(6) Das vollständige Antragspaket ist in den Akten abzulegen. Ein vollständiges Antragspaket besteht aus dem Antrag (Formblatt *AE Form 190-16A*), Kopien aller zur Ausstellung vorgelegten Dokumente, einer Kopie der Einleitung der Personenüberprüfung sowie ihrer Ergebnisse, dem Original der Anerkennung der Pflichten, dem *IACS*-Testausdruck, dem unterschriebenen Formblatt *AE Form 190-16E, Installation Pass Holder Consent Form* (nach Genehmigung abzurufen unter: <https://www.aeaim.hqusareur.army.mil/library/for/index.aef.shtm>) sowie der unterzeichneten Erklärung zum US-Datenschutzgesetz (*U.S Privacy Act*) (nur für US-Bürger). Wird Inhabern befristeter Kasernenausweise ein regulärer Ausweis ausgestellt, hat der ausstellende Mitarbeiter die für die Ausstellung erforderliche Mitteilung mit dem Originalantrag auf Ausstellung eines befristeten Kasernenausweises abzulegen.

b. Verfahren zur Ausstellung von Kasernenausweisen für Personen, die bereits im Besitz eines gültigen befristeten Ausweises sind, sind in Abs. 31 erläutert. Informationen zur Bearbeitung von Anträgen auf Erneuerung von Ausweisen, auf Ausstellung von Ausweisen als Ersatz gestohlener bzw. verlorengegangener Ausweise, auf Verlängerung befristeter Kasernenausweise sowie auf Ausstellung von Ausweisen als Ersatz für unbrauchbare Ausweise, s. Abs. 32 bis 35.

38. REGISTRIERUNG VON INHABERN EINER *DOD ID-CARD*

Zur Registrierung von Inhabern von *DOD ID-Cards* haben die Registratoren

a. zu überprüfen, welche Voraussetzungen Inhaber einer *DOD ID-Card* erfüllen müssen, um im *IACS* registriert zu werden;

b. den Inhaber einer *DOD ID Card* im *IACS* zu registrieren;

c. die vom Inhaber der *DOD ID-Card* unterzeichnete und datierte Erklärung zum US-Datenschutzgesetz (Anhang E) abzulegen.

39. DATENMÄSSIGE ERFASSUNG VON KINDERN

Eltern können Kinder unter 10 Jahren, die nicht im Besitz einer *DOD ID-Card* sind, unter Vorlage eines *Identi-Kids* datenmäßig erfassen lassen. Mit Hilfe des *Identi-Kid Kits* können dienende Informationen gesammelt werden, die der Identifizierung von Kindern dienen können: aktuelles Photo, Fingerabdrücke; Erkennungsmerkmale (wie Größe, Gewicht, Haarfarbe und Augenfarbe) sowie Namen von Personen, die zu benachrichtigen sind. Diese Informationen können von den Eltern und der Polizei bei der Suche nach verschwundenen, gekidnappten oder vermissten Kinder hernagezogen werden. Die Registratoren in den *IACOs* haben Kinder unter 10 Jahren, denen keine *DOD ID-Card* ausgestellt wurde, folgendermaßen zu erfassen:

a. Für jedes Kind ist Formblatt *AE Form 190-16D* (abrufbar unter: <https://www.aeaim.hqusareur.army.mil/library/for/index.aef.shtm>) ausgefüllt und unterschrieben zur Registrierung im *IACS* vorzulegen.

b. Die Registrierung hat in Anwesenheit eines Elternteils oder des gesetzlichen Vormunds zu erfolgen. Ein Kasernenausweis wird nicht ausgestellt.

40. BEARBEITUNG UND VERTEILUNG VON REGISTRIERUNGSLISTEN

a. Ausführliche Informationen zu den Registrierungslisten sind in Abs. 42 erläutert.

b. Die Bearbeitung und Verteilung von Registrierungslisten erfolgt über das zuständige *IACO*, soweit keine Ausnahmegenehmigung nach Abs. 42e(5) vorliegt

c. *IACO*-Registrierer haben

(1) sicherzustellen, daß alle Registrierungslisten gemäß den Vorgaben in Abs. 42 erstellt und bearbeitet werden;

(2) nach Einsatz- und Betriebsbereitschaft des *IACS* an den *ACPs* mit Hilfe des Moduls *Access Roster* die Registrierungslisten elektronisch zu bearbeiten und zu verteilen.

TEIL VI ZUGANGSFORMEN

41. EINTRAGUNG IN BESUCHERLISTEN

Die Möglichkeit der Eintragung von Personen in Besucherlisten dient dazu, Personen Zugang zu Einrichtungen der US-Streitkräfte im *USAREUR AOR* zu gewähren, wenn die Verwendung einer Registrierungsliste nicht erforderlich ist und die Ausstellung eines Kasernenausweises nicht erfolgen kann bzw. unzulässig ist.

a. Eintragung in Besucherlisten

(1) Inhaber von *DOD ID-Cards*, die Militärangehörige oder mindestens 18 Jahre und älter sind, sind berechtigt, Personen in Besucherlisten einzutragen. Ist diese Berechtigung aus irgendeinem Grund zeitweilig nicht zu gewähren, ist dies lediglich im *IACS* zu vermerken, nicht auf der *DOD ID-Card* selbst. Somit kann ein Wachposten den Entzug dieser Berechtigung nur feststellen, wenn er am *ACP* Zugriff zum *IACS* und damit die Möglichkeit zur Überprüfung der Daten des Ausweisinhabers hat. Inhaber von *DOD ID-Cards*, die nicht im *IACS* erfaßt sind, sind nicht berechtigt, Personen in Besucherlisten einzutragen.

(2) Mit Ausnahme Angehöriger der Personengruppe „NATO-Angehörige“ und „Mitarbeiter des US-Außenministeriums und der US-Botschaft“ wird Inhabern von Kasernenausweisen eine Berechtigung zum Eintragen von Personen in Besucherlisten nur gewährt, wenn dies von der *Sponsoring Organization* ausreichend begründet wird. Die Berechtigung wird im Rahmen der Erfassung im *IACS* gewährt und auf der Vorderseite des Ausweises vermerkt. Zusatzvermerke, wie z. B. „Ausschließlich Händler und Dienstleister“, sind in dem Feld „Bemerkungen“ auf der Rückseite des Ausweises einzutragen. Um die Berechtigung zum Eintragen von Personen in Besucherlisten zu erhalten, haben die Ausweisinhaber mindestens 18 Jahre alt zu sein. Inhaber befristeter Kasernenausweise erhalten keine Berechtigung zum Eintragen von Personen in Besucherlisten.

b. Einschränkungen

(1) Personen unter 18 wird keine Berechtigung zum Eintragen von Personen in Besucherlisten gewährt.

(2) Sowohl Inhaber von *DOD ID-Cards* wie auch Inhaber von Kasernenausweisen, die berechtigt sind, Personen in Besucherlisten einzutragen, dürfen zu keinem Zeitpunkt mehr als vier Personen mit ihren Fahrzeugen eintragen. Mehrfacheintragungen (auf mehreren Listen) zur Umgehung dieser Beschränkung sind unzulässig.

(3) Personen, die wiederholt Zugang zu Einrichtungen benötigen, dürfen sich nicht unter Umgehung des Antragsverfahrens zur Ausweisausstellung sowie der Anforderungen an Besucherlisten kontinuierlich in Besucherlisten eintragen lassen, um Zugang zu erhalten.

c. Sicherheitsstufenbezogene Beschränkungen. Bei Sicherheitsstufe Delta sind nur Inhaber von *DOD ID-Cards* berechtigt, Personen in Besucherlisten einzutragen.

d. Ausweisung

(1) In Besucherlisten eingetragene Personen haben den Wachposten ihren Reisepass bzw. Personalausweis vorzuzeigen (in Belgien die *Identity Card*, in Italien die *Carta d'Identita*). Die Wachen haben durch Gesichtskontrolle sicherzustellen, daß der Paß oder Personalausweis der eingetragenen Person auch gehört.

(2) Ist der *ACP* mit einem *IACS* ausgestattet, haben die Wachposten

(a) im Modul *Sign-in* die *DOD ID-Card* bzw. den Kasernenausweis des Eintragenden zu scannen. Wurde dem Eintragenden keine Berechtigung zum Eintragen von Personen in Besucherlisten gewährt, erscheint automatisch eine Warnmeldung auf dem Bildschirm. Eine Dateneingabe ist unter diesen Umständen gar nicht erst möglich;

(b) die Namen der Eingetragenen unter Beachtung der erlaubten Maximalzahl (s. vorstehenden Abs. b(2)) zu erfassen. Das *IACS* vergleicht automatisch die Namen der eingetragenen Besucher mit denen auf der Zugangsverbotsliste, um sicherzustellen, daß gegen die Eingetragenen kein Zugangsverbot verhängt wurde.

(3) Ist der *ACP* nicht mit einem *IACS* ausgestattet, hat aus der Ständigen Dienstanweisung für diesen Kontrollpunkt hervorzugehen, wie die Zugangsberechtigung eingetragener Personen zu überprüfen ist. Die aufgestellten Verfahren sollten sich weitgehend an die in vorstehendem Abs. (2) beschriebenen halten.

e. Aufgaben des Sponsors: Personen, die andere in Besucherlisten eintragen, haben die Handlungen dieser Personen zu überwachen und für deren Verhalten die Verantwortung zu übernehmen. Bei Nichteinhaltung der in diesem Abschnitt aufgestellten Vorgaben und Verfahren bzgl. der Eintragung von Personen in Besucherlisten kann die Eintragungsberechtigung entzogen werden.

42. REGISTRIERUNGSLISTEN

a. Registrierungslisten dienen dazu, Zugang zu Einrichtungen zu gewähren, wenn die Eintragung in Besucherlisten und die Ausstellung von Kasernenausweisen nicht praktikabel bzw. unzulässig sind.

b. Unbegrenzt gültige Registrierungslisten sind nicht zulässig. Registrierungslisten sind stets begrenzt gültig und dürfen nicht dazu verwendet werden, die Ausstellung von Ausweisen zu umgehen. Die Gültigkeit einer Registrierungsliste ist auf maximal 60 Tage begrenzt.

c. Registrierungslisten werden für einmalige bzw. nicht regelmäßig angesetzte Veranstaltungen erstellt. Sie sind in der Regel ortsgebunden und im Voraus zu koordinieren.

d. Die folgenden Beispiele sollen verdeutlichen, wann das Erstellen einer Registrierungsliste angebracht ist und wann nicht:

(1) Beispiel 1: Hat der Inhaber einer *DOD ID-Card* in einem Zeitraum von 3 Wochen vier Treffen mit mehreren ortsansässigen Vertretern (die noch in keiner Verbindung zu den US-Streitkräften stehen) zur Besprechung eines Vorhabens angesetzt, das möglicherweise auch Auswirkungen auf den Aufnahmestaat hat, wäre die Erstellung einer Registrierungsliste angebracht, da die Treffen nicht regelmäßig abgehalten werden, ortsgebunden sind und in einem Zeitraum von 60 Tagen stattfinden.

(2) Beispiel 2: Trifft sich eine zugelassene private Organisation (z.B. ein Tanzclub), zu der auch mehrere Mitglieder aus dem Aufnahmestaat gehören, regelmäßig mittwochs um 19:00 Uhr, ist das Erstellen einer Registrierungsliste nicht angebracht, da die Treffen regelmäßig stattfinden. Die ortsansässigen Mitglieder sind entweder jede Woche in Besucherlisten einzutragen oder haben gemäß den Vorgaben für "Mitglieder einer privaten Organisation" (Abs. 22) einen Kasernenausweis zu erhalten.

(3) Beispiel 3: Verpflichtet das *Directorate of Public Works* eine Privatfirma zur Durchführung von Bauarbeiten, die innerhalb eines Zeitraums von 2 Wochen abgeschlossen sind, ist die Erstellung einer Registrierungsliste angebracht, da der Vertrag nur über 2 Wochen läuft und die Vertragsausführung ortsgebunden ist.

(4) Beispiel 4: Plant der Inhaber einer *DOD ID-Card* in einer *Morale-Welfare-and-Recreation*-Einrichtung, seine Geburtstagsfeier abzuhalten und hat dazu 10 Personen eingeladen, die keine Zugangsberechtigung haben, ist die Erstellung einer Registrierungsliste angebracht, da es sich bei der Feier um eine einmalige Veranstaltung handelt und diese ortsgebunden ist.

e. Die Bearbeitung und Verteilung von Registrierungslisten hat nach folgenden Verfahren zu erfolgen:

(1) Nur im *IACS* registrierte Inhaber einer *DOD ID-Card* können die Ausstellung einer Registrierungsliste beantragen und den entsprechenden Antrag unterschreiben. Unter Abfrage der im *IACS* gespeicherten Daten haben *IACO*-Registrierer sicherzustellen, daß die beantragende Person im Besitz einer *DOD ID-Card* und im *IACS* erfaßt ist.

(2) Das Original eines Antrags auf Erstellung einer Registrierungsliste ist persönlich beim zuständigen *IACO* abzugeben oder per E-Mail zu übermitteln. Wird der Antrag per E-Mail übermittelt, ist sicherzustellen, daß die E-Mail-Adresse eine militärische Kennung („*mil*“) oder die Kennung „*gov*“ oder „*org*“ hat sowie den Namen des Absenders enthält, der den Antrag unterzeichnet hat (z.B. *john.smith@us.army.mil*). Der Erhalt der E-Mail ist von dem für die Ausweisausstellung zuständigen Mitarbeiter des *IACO* zu bestätigen. Per Fax übermittelte Anträge auf Erstellung einer Registrierungsliste sind unzulässig. Eine vollständige Liste aller zugelassenen *IACOs* kann unter <http://www.hqusareur.army.mil/opm/iacs/Resources/USAREURACSRRegistrationStations.pdf> abgerufen werden.

(3) Anträge auf Erstellung von Registrierungslisten sind mindestens 3 Arbeitstage vor dem Datum, ab dem die Liste gelten soll, einzureichen, damit den *IACO*-Registrierern ausreichend Zeit für die Erstellung und Bearbeitung der Liste bleibt.

(4) Die Registrierungslisten haben folgende Angaben zu enthalten:

(a) vollständiger Name, Staatszugehörigkeit, Reisepass- bzw. Personalausweisnummer (d.h. die Nummer eines der unter Abs. 30d(1) aufgeführten Dokumente; dieses Dokument ist dem Wachposten vor Zugangsgewährung vorzuzeigen). Diese Angaben sind für alle auf der Liste aufgeführten Personen zu machen. Werden von diesen Personen Fahrzeuge mitgeführt, so ist außerdem das Kennzeichen des mitgeführten Fahrzeugs anzugeben;

(b) Gültigkeitsbeginn und -ende. Zwischen beiden Daten dürfen nicht mehr als 60 Tage liegen;

(c) Begründung des Antrags und Ort, an dem die Veranstaltung stattfindet bzw. an dem die Arbeit ausgeführt wird, sowie die *ACPs*, an denen die Registrierungsliste gelten soll. Für Anträge auf Ausstellung großangelegter Registrierungslisten (z. B. für Großtransporte) sind Angaben wie „*USAREUR*-weit“ oder „*98th ASG*-weit“ zulässig. Eine solch liberale Zugangsberechtigung sollte allerdings nur beantragt werden, wenn dies aus operativen Gründen erforderlich ist. Ziel des *Installation Access Control Programs* ist es nämlich, den Zugang auf die geringstmögliche Anzahl von Einrichtungen zu beschränken. Organisationen haben die Registrierungslisten nicht zur Umgehung der Vorgaben, den Zugang auf ein Minimum zu beschränken, aus reiner Bequemlichkeit zu verwenden;

(d) Wird die Liste für eine vertraglich verpflichtete Privatfirma oder einen Lieferservice erstellt, sind Firmenname und Telefonnummer anzugeben;

(e) Wird die Liste für einen Lieferservice erstellt, sind die Tage und Zeiten, an/zu denen die Lieferungen erfolgen, anzugeben (z.B. Montags zwischen 7:00 und 16:00);

(f) Wird für Mitarbeiter verpflichteter Privatfirmen oder Dienstleister eine Registrierungsliste erstellt (z. B. für einen Baurupp, Lieferservice), so sind ein polizeiliches Führungszeugnis vorzulegen und die Vorgaben bzgl. der Vorlage einer Arbeits- und Aufenthaltserlaubnis einzuhalten. Diese Dokumente sind dem Antrag auf Erstellung einer Registrierungsliste beizufügen. Wird der Antrag per E-Mail gestellt, hat der Antragsteller auf dem Antrag zu vermerken, daß ein Führungszeugnis vorliegt und die Voraussetzungen bzgl. einer Arbeits- und Aufenthaltserlaubnis erfüllt sind.

(5) Ist die Gültigkeit einer Registrierungsliste auf eine Einrichtung beschränkt, kann mit Genehmigung des *BSB* die Bearbeitung und Verteilung der Registrierungsliste durch bestimmte Personen erfolgen, die diese Einrichtung vertreten (z. B. *Installation Coordinator*). Die *BSBs* haben sicherzustellen, daß diese Verfahren in den Ständigen Dienstanweisungen und in speziellen Anordnungen für Wachposten erläutert sind.

(6) Die *BSBs* haben durch Festlegung entsprechender Verfahren sicherzustellen, daß

(a) die Namen der auf der Registrierungsliste aufgeführten Personen mit den Namen derer, für die ein Zugangsverbot zu *USAREUR*-Einrichtungen verhängt wurde, verglichen werden und die aufgrund ihrer Staatszugehörigkeit geltenden Voraussetzungen bzgl. einer evtl. erforderlichen Aufenthalts- und Arbeitserlaubnis erfüllt sind;

(b) durch einen entsprechenden Vermerk auf den Registrierungslisten hervorgeht, daß sie vom *BSB* vor Verteilung genehmigt wurden;

(c) genehmigte Registrierungslisten vor Beginn ihrer Gültigkeit an den entsprechenden *ACPs* ausgelegt bzw. abgeheftet sind.

f. Folgende Vorgehensweisen sind von den Wachposten zu beachten:

(1) Informiert eine Person bei Ankunft am *ACP* den Wachposten, daß sie auf einer Registrierungsliste steht, hat der Wachposten den Reisepass oder Personalausweis zu verlangen (notwendigerweise eines der in Abs. 30d(1) aufgelisteten Dokumente) und die Nummer des Dokuments mit der auf der Registrierungsliste geführten Nummer zu vergleichen. Diese Nummern müssen übereinstimmen.

(2) Der Wachposten hat den Zugang zu verweigern, wenn die Person nicht auf der Registrierungsliste steht, die Angaben auf dem Reisepass oder Personalausweis nicht mit den Angaben auf der Registrierungsliste übereinstimmen oder die Registrierungsliste abgelaufen ist.

(3) Wurde die Registrierungsliste zur Anlieferung von Waren erstellt, haben die Wachposten die Lieferscheine bzw. Frachtbriefe zu überprüfen und sicherzustellen, daß der Anlieferungsort angegeben ist.

(4) Wird Zugang gewährt, führen die Wachen eine Untersuchung der Personen, Taschen und Fahrzeuge gemäß den örtlich geltenden Dienstanweisungen durch.

g. Nach Einsatz- und Betriebsbereitschaft des *IACS* an den *BSB ACPs* hat die Bearbeitung und Verteilung von Registrierungslisten elektronisch mit Hilfe des Moduls *Access Roster* zu erfolgen.

(1) Die *IACO*-Registrierer haben die auf der Registrierungsliste gemachten Angaben ins *IACS* zu übertragen und einen Ausdruck des Antrags auf Erstellung einer Liste abzulegen, damit diese nach Bedarf verteilt werden kann.

(2) Die Wachposten haben nach den Vorgaben in vorstehendem Buchstaben f vorzugehen, haben allerdings die Überprüfung durch manuelle Abfrage im *IACS* durchzuführen und nicht anhand eines Ausdrucks der Registrierungsliste.

43. EINFAHRT VON EINSATZ- UND RETTUNGSFAHRZEUGEN

Nachstehende Verfahren sollen *BSB*-Kommandeuren als Vorgaben für die Einfahrt von Einsatz- und Rettungskräften und -fahrzeugen (z. B. der Polizei, der Feuerwehr, der medizinischen Notfallversorgung oder des Personenschutzes) dienen:

a. Zugang in Notfallsituationen

(1) Einsatz- und Rettungsfahrzeuge (sowohl US als auch aus dem Aufnahmestaat) sind nicht unnötig aufzuhalten, so sie eindeutig als Einsatz- oder Rettungsfahrzeuge mit Sirene und eingeschaltetem Blaulicht erkennbar sind. Die Fahrzeuginsassen haben sich allerdings mittels eines gültigen Ausweises auszuweisen und das Fahrzeug ist flüchtig zu durchsuchen, bevor die Erlaubnis zur Einfahrt in die Einrichtung erteilt wird.

(2) *BSB*-Kommandeure sollten in Zusammenarbeit mit den örtlichen Rettungsdiensten des Aufnahmestaates Verfahren zur Meldung von Notfällen festlegen. Dabei ist festzulegen, dass bei der Meldung der *ACP* anzugeben ist, an dem eingefahren wird. Ausserdem ist festzulegen, wie die Meldung der Notfall-/Rettungsdienste an das *PMO* und die Mitteilung des *PMO* an die *ACPs* über einfahrende Notfall-/Rettungsdienste auszusehen hat und welche Angaben zu machen sind.

(3) Die *BSBs* haben zu verlangen, daß Einsatz- und Rettungsfahrzeuge kurz anhalten, damit die Identität des Fahrers und der anderen Fahrzeuginsassen überprüft, eine flüchtige Überprüfung des Innenraums des Fahrzeugs erfolgen und der Unfallort festgestellt werden kann. Bei einer flüchtigen Durchsuchung ist der Innenraum eines Fahrzeugs sowie die Ladefläche bzw. des Kofferraums zu untersuchen.

ANMERKUNG: Einsatz- und Rettungsfahrzeuge sollten so kurz wie möglich (in der Regel nie länger als 30 Sekunden) angehalten werden. Die Rettungsdienste sind im Vorfeld entsprechend zu informieren, damit sie über die Notwendigkeit der Zugangskontrolle in Notfällen aufgeklärt sind. Die Notfall-/Rettungsdienste sind durch eine von den US-Militärpolizeidienststellen dazu bestimmte Person zu begleiten. Dabei ist die Regelhaltezeit dieser Fahrzeuge von maximal 30 Sekunden zu beachten.

b. Polizeikräfte der US-Streitkräfte: Polizeikräfte der US-Streitkräfte (US-Militärpolizei, USAFE-Sicherheitskräfte) in als entsprechend gekennzeichneten Militärpolizeifahrzeugen und in Uniform haben sich auszuweisen. Polizeikräfte der US-Streitkräfte in Zivil (z. B. Ermittlungsbeamte und Beamte der Kriminalpolizei) bzw. in nicht als Militärpolizeifahrzeug gekennzeichneten Kraftfahrzeugen haben sich ordnungsgemäß auszuweisen und sich an die üblichen Verfahren zur Zugangskontrolle zu halten, es sei denn es liegt ein Notfall vor.

c. Polizeikräfte des Aufnahmestaates

(1) Polizeikräfte des Aufnahmestaates in als Polizeifahrzeug gekennzeichneten Fahrzeugen und in Uniform haben sich bei der Einfahrt in US-Einrichtungen auszuweisen.

(2) Bei Notfalleinsätzen der deutschen Polizei sind die Anweisungen in a oben zu befolgen.

(3) Polizeikräfte des Aufnahmestaates, die nicht in entsprechend gekennzeichneten Fahrzeugen einfahren und nicht in Uniform sind, haben sich auszuweisen (z. B. mit einem Reisepass, Personalausweis oder einem Polizeiausweis. Der Polizeiausweis muß auf sie ausgestellt sein, ihr Photo und eine der folgenden Bezeichnungen auf der Vorderseite aufweisen: Polizei Dienstausweis, Zollpolizei Dienstausweis, Kriminalpolizei Dienstausweis). Die 22d und 80th ASG sollten eine Beschreibung der Ausweise der Polizei des Aufnahmestaates in ihre Ständigen Dienstanweisungen aufnehmen. Sollten berechnigte Zweifel an der Gültigkeit der Ausweise oder an der Notwendigkeit des Zugangs zur Einrichtung bestehen, hat der Wachposten die Polizeikräfte der US-Streitkräfte (z.B. die US-Militärpolizei) zu verständigen.

(4) Polizeibeamten des Aufnahmestaates, die mit den Polizeikräften der US-Streitkräfte in einer Einrichtung zusammenarbeiten, kann zur Erleichterung des Zugangs zur Einrichtung ein Kasernenausweis der Kategorie "Offizielle Gäste" (Abs. 25) ausgestellt werden.

d. Feuerwehr: Feuerwehrleuten, die bei den US-Streitkräften beschäftigt sind, sollte ein Kasernenausweis der Kategorie „Ortsansässige Arbeitnehmer“ (Abs. 13) ausgestellt werden. Mitglieder der Feuerwehr des Aufnahmestaates sollten nur in Notfällen Zugang zu Einrichtungen haben.

e. Medizinische Notfallversorgung: Die medizinische Notfallversorgung erfolgt durch die örtlichen Krankenhäuser des Aufnahmestaates. Rettungs- und Krankenwagen fahren bei Notfällen in der Regel mit Sirenen und Blaulicht in Einrichtungen ein. Sie sind unter diesen Umständen nicht über Gebühr anzuhalten (s. vorstehenden Buchstaben a). Krankenwagen sind in Deutschland durch eine der folgenden Aufschriften eindeutig gekennzeichnet: „Ambulance“, „Krankenwagen“ oder „Notarzt“. Die Ständigen Dienstanweisungen der 22d und 80th ASG sollten eine Beschreibung der Krankenwagen des Aufnahmestaates enthalten.

f. Andere Dienstleister des Aufnahmestaates: Für andere Dienstleister des Aufnahmestaates, die in nicht-lebensbedrohlichen Notfällen Hilfe leisten (z. B. Mitarbeiter der Wasserwerke, Stromgesellschaften oder Heizungsfirmen) sind von den BSBs alternative Verfahren zur Zugangskontrolle aufzustellen. In diesen Fällen ist kein ungehinderter Zugang zu gewähren. Die BSBs sollten schriftlich in einem *Memorandum of Agreement* mit diesen Dienstleistern übereinkommen, daß diese die Einrichtung rechtzeitig im Voraus benachrichtigen, wenn Zugang erforderlich ist.

g. Fahrzeuge des Personenschutzes:

(1) Gepanzerte Personenschutz-Fahrzeuge und Fahrzeuge des Begleitschutzes sind nicht generell und unbeschränkt berechnigt, in bewachte Einrichtungen ohne Vorlage der entsprechenden Genehmigung einzufahren.

(2) Erkennen die Wachposten am ACP das gepanzerte Fahrzeug und seinen Führer, so können sie darauf verzichten, das gepanzerte Fahrzeug anzuhalten, und können das Fahrzeug und seine Insassen passieren lassen.

(3) Lediglich der Führer eines gepanzerten Fahrzeuges hat seine *DOD ID-Card* vorzuzeigen (Einsatz-Anforderung, Führerschein oder andere Papiere sind nicht vorzuzeigen.). Ausnahmeregelungen sind für jede Einrichtung gesondert zu treffen und müssen vom ASG Kommandeur genehmigt sein. Eine Aufforderung an die anderen Fahrzeuginsassen, sich auszuweisen, darf nicht erfolgen.

(4) Zur Überprüfung des Ausweises des Fahrzeugführers dürfen Wachposten lediglich verlangen, dass das Fenster auf der Fahrerseite geöffnet wird. Die Wachposten haben keine Überprüfung des Innenraums vorzunehmen, die Fahrzeuginsassen nicht zum Aussteigen aufzufordern oder Anstalten zu treffen, das Fahrzeug zu durchsuchen.

(5) Wird ein gepanzertes Fahrzeug von einem zweiten Fahrzeug begleitet, ist lediglich der Ausweis des Fahrers des vorausfahrenden Fahrzeuges zu kontrollieren. Dieser hat die Wachen zu informieren, daß es sich beim nachfolgenden Fahrzeug um ein Begleitfahrzeug handelt. Ziel ist es, diese Fahrzeuge so schnell wie möglich passieren zu lassen ohne Umgehung umsichtiger Sicherheitsvorkehrungen.

ANMERKUNG: BSB-Kommandeure sind berechnigt, alternative Verfahren aufzustellen bzw. vorstehende Vorgaben je nach herrschender Sicherheitsstufe abzuändern.

44. ACP-WACHPOSTEN

a. ACP-Wachposten haben

(1) gemäß dieser Dienstvorschrift und *AE-Regulation 190-13* ihren Dienst zu versehen;

(2) nur jenen Personen Zugang zu gewähren, die gemäß den in dieser Dienstvorschrift vorgegebenen Richtlinien und Verfahren eine Zugangsberechtigung haben. Die Zugangsberechtigung aller Personen, die eine bewachte Einrichtung der US-Streitkräfte betreten, ist zu überprüfen. Bei Einfahrt mit Fahrzeugen ist die Berechtigung aller Fahrzeuginsassen (nicht nur die des Fahrers) zu überprüfen.

(3) sich an die Vorgaben bzgl. der Eintragung von Personen in Besucherlisten in Abs. 41 und denen bzgl. der Erstellung, Bearbeitung und Verteilung von Registrierungslisten in Abs. 42 zu halten;

(4) die Militärpolizei zu benachrichtigen, wenn eine *DOD ID-Card* bzw. ein Kasernenausweis abgelaufen ist oder sie/er unbrauchbar ist und nicht mehr zur Überprüfung der Zugangsberechtigung herangezogen werden kann. Personen, deren unbrauchbare(r) *ID-Card* bzw. Kasernenausweis eingezogen wurde, kann Zugang gewährt werden, wenn sie im *IACS* erfaßt und zugangsberechtigt sind (s. nachstehende Buchstaben g und h). Personen, deren Ausweis eingezogen wurde und deren Identität mit Hilfe des *IACS* nicht festgestellt werden kann, ist kein Zugang zu gewähren, es sei denn, sie werden von einem dazu Berechtigten in eine Besucherliste eingetragen.

ANMERKUNG: *DOD ID-Cards* bzw. Kasernenausweise können von allen den Zugang Kontrollierenden unter Verwendung von Formblatt *AE Form 190-16B* eingezogen werden. Gemäß der Vorgaben in Abs. 5g(1)(b) haben die *BSBs* unter Festlegung entsprechender Verfahren sicherzustellen, daß den Betroffenen eine Bescheinigung über den Einzug und Empfang ausgestellt und die eingezogenen Dokumente beim zuständigen *IACO* bzw. der Ausweis-ausstellenden Stelle abgegeben werden. Aufgrund einer Bescheinigung über den Einzug bzw. den Ablauf einer *DOD ID-Card* bzw. eines Kasernenausweises ist nie Zugang zu gewähren.

b. Kann das *IACS* zur Überprüfung der Zugangsberechtigung nicht herangezogen werden, müssen die Wachposten in der Lage sein, die Zugangsberechtigungsdokumente manuell zu überprüfen. Aufgrund entsprechender örtlich geltender Vorgaben kann die Vorlage eines zweiten Ausweises und des Fahrzeugscheins verlangt werden (z. B. gründliche Untersuchung von Personen und Fahrzeugen im Rahmen bestimmter sicherheitsstufenbedingter oder Anti-Terror-Maßnahmen). Für diese manuelle Überprüfung haben die *BSBs* entsprechende Vorgaben aufzustellen und diese in einschlägige Vorschriften und Ständige Dienstanweisungen aufzunehmen.

c. Ist das *IACS* an einem *ACP* verfügbar und einsatz- und betriebsbereit, haben die Wachposten die Überprüfung der *DOD ID-Cards* und der Kasernenausweise ausschließlich durch Scannen der Ausweise durchzuführen, es sei denn die manuelle Überprüfung ist vorübergehend aufgrund operativer Erfordernisse als zusätzliche Kontrolle notwendig. Dies führt zu einer eindeutigen Überprüfung der Zugangsberechtigung der Ausweisinhaber. Eine Überprüfung anderer Dokumente (z. B. eines zweiten Ausweises oder des Fahrzeugscheins) ist nicht erforderlich, wenn der Ausweisinhaber im *IACS* erfaßt und zugangsberechtigt ist.

ANMERKUNG: Das volle Potential des *IACS* kann nur ausgeschöpft werden, wenn das System konsequent und lückenlos eingesetzt wird.

d. Wird beim Scannen eines Kasernenausweises festgestellt, daß sein Inhaber nicht im *IACS* registriert ist, sollten die Wachen das Ausstellungsdatum überprüfen. Am selben Tag ausgestellte Kasernenausweise sind möglicherweise noch nicht in der *IACS*-Datenbank gespeichert. In örtlich geltenden Dienstanweisungen ist festzulegen, unter welchen Voraussetzungen Inhabern von Kasernenausweisen, denen erst ein Ausweis ausgestellt wurde und die deshalb möglicherweise noch nicht im *IACS* erfaßt sind, Zugang gewährt werden kann. Liegt die Ausstellung des Ausweises allerdings länger als einen Tag zurück ist, ist die zuständige Militärpolizei zu benachrichtigen, damit diese den Ausweis einzieht und seine Gültigkeit überprüft.

e. Personen, die im Besitz einer gültigen *DOD ID-Card*, aber nicht im *IACS* registriert sind, kann nur mit ausdrücklicher Genehmigung des *BSB*-Kommandeurs bzw. einer übergeordneten Stelle der Zugang verweigert werden. Bei diesen Personen handelt es sich in der Regel um Personen, die auf Dienststreife, abkommandiert oder neu dem Kommando unterstellt sind. Die Wachposten haben in diesen Fällen

(1) nicht im *IACS* erfaßte Inhaber einer *DOD ID-Card* anzuweisen, sich umgehend im *IACS* registrieren zu lassen;

(2) diese nicht-registrierten Inhaber einer *DOD ID-Card* in das *IACS* einzugeben, um deren Zugang zu erfassen. Diese Notwendigkeit kann für die Inhaber von *DOD ID-Cards* zu geringen Verzögerungen beim Zugang führen und so ein Anreiz sein, sich bei nächster Gelegenheit im *IACS* registrieren zu lassen. Inhaber von *DOD ID-Cards*, die nur für kurze Zeit Zugang zu einer Einrichtung der US-Streitkräfte benötigen (z. B. zum Besuch eines Softballspiels am Wochenende) müssen in der Regel nicht im *IACS* registriert werden. Wenn sich der Inhaber einer *DOD ID-Card* gerade erst im *IACS* hat registrieren lassen, die örtliche Datenbank aber noch nicht aktualisiert wurde, haben die Wachposten diese Person wie einen nicht registrierten Inhaber einer *DOD ID Card* zu behandeln.

(3) die Überprüfung anderer Dokumente (z. B. eines zweiten Ausweises oder des Fahrzeugscheins) gemäß den örtlich geltenden Richtlinien und Dienstanweisungen durchzuführen;

ANMERKUNG: Inhabern von *DOD ID-Cards*, die nicht im *IACS* erfaßt sind, ist die Berechtigung zum Eintragen von Personen in Besucherlisten nicht zu gewähren.

f. *BSB*-Kommandeure haben sicherzustellen, daß die in vorstehendem Abs. e vorgeschriebenen Verfahren in spezielle Anweisungen für Wachposten als bindend aufgenommen werden.

g. Kann eine *DOD ID-Card* oder ein Kasernenausweis nicht gescannt werden (weil z. B. der Strichcode nicht lesbar ist), der Inhaber des Ausweises aber angibt, im *IACS* registriert zu sein, können die Wachposten anhand der an ihrem Arbeitsplatz im Wachhäuschen verfügbaren Unterlagen die Zugangsberechtigung des Ausweisinhabers überprüfen. Inhabern einer *DOD ID-Card* und Inhabern eines Kasernenausweises, die, wie eindeutig festgestellt wird, im *IACS* registriert sind, ist Zugang zu gewähren. Sie sind anzuweisen, sich umgehend eine neue *DOD ID-Card* bzw. einen neuen Kasernenausweis ausstellen zu lassen. Wird bei der Überprüfung der verfügbaren Unterlagen festgestellt, daß ein Ausweisinhaber nicht im *IACS* erfaßt ist oder der Ausweisinhaber angibt, nicht im *IACS* erfaßt zu sein, haben sich die Wachen bei Inhabern von Kasernenausweisen an die Vorgaben in vorstehendem Abs. d und bei Inhabern von *DOD ID-Cards* an die in vorstehendem Abs. e zu halten.

h. Die Überprüfung der Zugangsberechtigung von Inhabern von *DOD ID-Cards* bzw. von Kasernenausweisen, die ihren Ausweis vergessen haben, kann nach Genehmigung der *BSB*-Kommandeure durch manuelle Abfrage im *IACS* bzw. durch Fingerabdruckvergleich erfolgen, um ihnen Zugang gewähren zu können und nicht verweigern zu müssen.

i. Mitarbeitern privater Wachdienste, die bei *USAREUR* als Wachposten beschäftigt sind, wird aufgrund dieses Beschäftigungsverhältnisses nicht automatisch ein Kasernenausweis ausgestellt. Sie haben sich

(1) auf Besucherlisten einzutragen oder in Registrierungslisten aufzunehmen zu lassen, wenn Zugang nicht wiederholt erforderlich ist (z.B. sondern nur zu Schulungszwecken).

(2) einen Kasernenausweis ausstellen zu lassen, wenn sie aufgrund ihrer Position oder ihres Dienstorts wiederholt Zugang zu Einrichtungen benötigen. Dabei sind sie als Angehöriger der Gruppe der „Mitarbeiter verpflichteter Privatfirmen (im Aufnahmestaat lebend)“ (Abs. 15) zu behandeln.

(3) im *IACS* registrieren zu lassen, damit sie während ihres Wachdienstes an einem mit einem betriebsbereiten *IACS* ausgestatteten *ACP* die Voraussetzungen zur Anmeldung im *IACS* als Nutzer erfüllen. Mitarbeiter privater Wachfirmen ist als „Wachposten“ (Abs. 29) zur Erfassung im *IACS* ein Kasernenausweis auszustellen, damit sie sich als *IACS*-Nutzer anmelden können.

ANHANG A BEZUGSDOKUMENTE

TEIL I VORSCHRIFTEN

Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons

Public Law 106-246, Military Construction Appropriations Act, 2001

Privacy Act, 1974

5 USC 552a(b), Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings

10 USC 3013, Secretary of the Army

10 USC 5013, Secretary of the Navy

10 USC 8013, Secretary of the Air Force

Zusatzabkommen zum NATO-Truppenstatut

DOD Directive 8500.1, Information Assurance (IA)

AR 190-13, The Army Physical Security Program

AR 190-56, The Army Civilian Police and Security Guard Program

AR 381-45, Investigative Records Repository

AR 25-2, Information Assurance

AR 600-8-14, Identification Cards for Members of the Uniformed Services, Their Family Members, and Other Eligible Personnel

Technical Manual 5-853-2, Security Engineering Concept Design

AE Regulation 190-1, Registering and Operating Privately Owned Motor Vehicles in Germany

AE Regulation 190-13, The USAREUR Physical Security Program

AE Regulation 525-13, Antiterrorism/Force Protection: Security of Personnel, Information, and Critical Resources

USAREUR Regulation 600-700, Identification Cards and Individual Logistic Support

USAREUR Regulation 604-1, Foreign National Screening Program (Laredo Leader)

USAREUR Regulation 690-64, Local National Employee Conduct, Discipline, Complaints, Grievances, and Labor Disputes

TEIL II FORMBLÄTTER

SF 50-B, Notification of Personnel Action

DD Form 2(ACT), Armed Forces of the United States Geneva Convention Identification Card (Active)

DD Form 2(RET), United States Uniformed Services Identification Card (Retired)

DD Form 2(RES), Armed Forces of the United States Geneva Convention Identification Card (Reserve)

DD Form 2(RES RET), Armed Forces of the United States Identification Card (Reserve Retired)

DD Form 1172, Application for Uniformed Services Identification Card—DEERS

DD Form 1173, United States Uniform Services Identification and Privilege Card (Dependent)

DD Form 1173-1, United States Uniformed Services Identification and Privilege Card (Reserve Dependent)

DD Form 1934, Geneva Convention Identity Card for Medical and Religious Personnel Who Serve in or Accompany the Armed Forces

DD Form 2765, Department of Defense/Uniformed Services Identification and Privilege Card

DA Form 31, Request and Authority for Leave

DA Form 2028, Recommended Changes to Publications and Blank Forms

DA Form 3434, Notification of Personnel Action - Nonappropriated Funds Employee

AE Form 190-16A, Application for USAREUR/USAFE Installation Pass

AE Form 190-16B, Receipt for Confiscated ID Card

AE Form 190-16C, Record of Destruction

AE Form 190-16D, IACS Identi-Kid Permission Slip

AE Form 190-16E, IACS Installation Pass Holder Consent Form

AE Form 600-700A, USAREUR Privilege and Identification Card

AE Form 604-1B, Personnel Data Worksheet

ANHANG B
BESTELLUNG DER SPONSORING OFFICIALS (MUSTERSCHREIBEN)

Appropriate Letterhead			
Office Symbol	Date		
MEMORANDUM FOR <i>(enter the name of the servicing IACO)</i>			
SUBJECT: Designation of Sponsoring Officials			
1. The following individuals are designated as sponsoring officials for <i>(enter the name of the organization)</i> :			
a. Authorized to grant up to U.S. Forces-wide access <i>(minimum LTC/GS-13/C-8/NF 5)</i>			
FULL NAME	POSITION	GRADE	OFFICIAL E-MAIL ADDRESS
b. Authorized to grant up to ASG-wide access <i>(minimum SGM/CSM/MAJ/CW4/GS-12/C-7A/NF 4)</i> :			
FULL NAME	POSITION	GRADE	OFFICIAL E-MAIL ADDRESS
c. Authorized to grant up to BSB-wide access <i>(minimum ISG/MSG/CW3/CPT/GS-11/C-7/NF 4)</i> :			
FULL NAME	POSITION	GRADE	OFFICIAL E-MAIL ADDRESS
d. Authorized to grant access for only one installation <i>(minimum SFC/CW2/GS-9/C-6A)</i> :			
FULL NAME	POSITION	GRADE	OFFICIAL E-MAIL ADDRESS
2. The POC for this information is <i>(include name, telephone number, and e-mail address)</i> .			
Signature block of commander or designated official <i>(commander or first LTC/GS-13 in the chain of command)</i>			

ANHANG C
FORMBLATT AE FORM 190-16A (MUSTER)

APPLICATION FOR USAREUR/USAFE INSTALLATION PASS (AE Reg 190-16)						
Data required by the Privacy Act of 1974						
Authority: Article 53, Supplementary Agreement to NATO SOFA; 10 USC 3012.						
Principal purpose(s): For identification of U.S. and non-U.S. nationals employed by U.S. Government agencies, contractors, and vendors of non-military agencies of countries in which U.S. personnel have been accommodated when these personnel require recurring access to the accommodations under U.S. control and do not possess other valid entry authorization documents.						
Routine use(s): To identify personnel authorized routine or recurring access to installations under U.S. control.						
Mandatory or voluntary disclosure and effect on individual not providing information: Voluntary. However, failure to provide any item of information will result in denial of entry onto the U.S.-controlled installations for which the AE Form 190-16A has been validated.						
Please refer to the instructions on page 3 to ensure that the form is correctly filled in.						
1. To 293d BSB, IACO Mannheim		2. From 5th Signal Command, Mannheim			3. Date (mm/dd/yyyy) 12/01/2004	
4. Applicant name (Last, first, MI) SCHMIDT, HANS L.		5. Sponsor address 5th Sig Cmd (NETC-SOP) CMR 420 APO AE 09056-0420		6. Address (Company/Organization/Unit) 5th Sig Cmd (NETC-SOP) CMR 420 APO AE 09056-0420		
7. Person category Local National Employee		8. Country of citizenship Germany		9. SSN/Personal ID number 6475611633		
10. Supporting document expiration date (Passport/ID card) (mm/dd/yyyy) 01/15/2006		11. Residence permit <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No		12. Work permit <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No		
13. Type pass requested <input checked="" type="checkbox"/> Installation pass <input type="checkbox"/> Temporary installation pass	14. Date of birth (mm/dd/yyyy) 11/17/1964	15. Weight (Pounds) 170	16. Height (Inches) 71	17. Eye (Color) Blue	18. Hair (Color) Brown	
19. Installations for which access is required USAREUR-wide (Germany only)						
20. Limitations/time/day access is required 24/7		21. FPCON restriction DELTA		22. Pass expiration date (mm/dd/yyyy) 01/15/2006 IACO REGISTRAR MUST VALIDATE		23. Sign-in privileges <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
24. Privately owned vehicle (POV) registration information (additional vehicles may be added on a separate sheet of paper)						
a. License number	b. Country	c. Make	d. Model	e. Year	f. Body type	g. Color
MA-T123	Germany	Ford	Ka	2003	2-door	White
25. Company name and telephone number						
26. Verification by sponsoring official (must check both boxes)						
<input checked="" type="checkbox"/> I have reviewed the results of all background checks required by AE Reg 190-16 and verify that there is no derogatory information that would preclude the issuing of an installation pass.						
<input checked="" type="checkbox"/> I verify that the applicant has been informed about the purpose and proper use of the installation pass. I have reviewed AE Reg 190-16 and believe this packet is administratively correct, and fully and accurately reflects the applicant's access requirements. However, if there is a problem or you need further information please contact me.						
a. Organization and telephone number 5th Signal Command DSN 381-9303			b. Name and title COL Bill B. Brown, G-3			
c. Signature			d. Date (mm/dd/yyyy)			
27. To be completed by registrar						
a. Registrar name			b. Date issued			

28. Installation for which access is required (Provide justification)

Mr. Schmidt's job involves conducting network infrastructure surveys in support of all the signal battalions in Germany. This requires him to travel to all the ASGs in Germany, hence USAREUR-wide access (Germany only) is required.

29. Sign-in privileges (Provide justification)

While conducting network infrastructure surveys, Mr. Schmidt must coordinate with and involve host nation telecommunications experts to ensure that DOD does not violate host nation laws and statutes. This requirement necessitates that Mr. Schmidt be able to sign on these people to accomplish his mission.

Required attachments (Check applicable boxes)

Requirements may be different depending on the person category selected. All installation-pass applications must include supporting documents. Some installation-pass applications may include a copy of:

- | | |
|--|--|
| <input type="checkbox"/> Residence permit | <input type="checkbox"/> Defense Clearance Investigation Index (DCII) |
| <input type="checkbox"/> Work permit | <input checked="" type="checkbox"/> Proof of AE Form 604-1A, Foreign National Screening (FNS), initiation/completion |
| <input checked="" type="checkbox"/> Police Good Conduct Certificate (PGCC)
(<i>Polizeiliches Führungszeugnis</i>) | <input checked="" type="checkbox"/> Military police (MP) check results |

Instructions for completing AE Form 190-16A

Item 1. To

Enter the name of the servicing installation access control office.

Item 2. From

Enter the name of the sponsoring official's organization.

Item 5. Sponsor address

Enter the mailing address of the sponsoring organization. For the person categories Personal-Service Employee, Visitor (immediate family member living in Europe), and Visitor (friend or family member not included in the "immediate family member living in Europe)" category, also include the requester's mailing address.

Item 6. Address

Enter the address of the unit of assignment. This address will depend on the applicant's person category. For example, for local national employees, enter the hiring organization's address. For Contractors and Delivery Personnel, enter the address of their company. Visitors should list their home mailing address.

Item 7. Person category

- DOD ID-card holder
- Local national employee
- Contractor (based in United States)
- Contractor (living in host nation)
- Personal-service employee
- Delivery personnel (recurring deliveries or similar service not associated with a Government contract)
- Vendor or commercial solicitor
- NATO member
- Host-nation military member
- Foreign student (Marshall Center)
- Member of private organization
- Visitor (immediate family member living in Europe)
- Visitor (friend or family member not included in category above)
- Official guest
- Department of State and American Embassy personnel
- Other
- Host-nation Government official
- Gate guard

Item 9. SSN/Personal ID number

Enter the personal ID number or the passport number from the supporting document used. Applicant must have one of the following supporting documents:

- Passport
- Personal ID card issued by the country of citizenship (for example, German *Personalausweis*, Belgian identity card, Italian *carta d'identità*)
- Military ID card issued by one of the NATO Sending States (Belgium, Canada, France, the Netherlands, United Kingdom)

Item 10. Supporting document expiration date

Enter the expiration date of the supporting document (for example, expiration date of passport or German *Personalausweis*).

Item 11. Residence permit

If required, check the appropriate box to indicate whether a copy of the residence permit is attached. See AE Reg 190-16 for guidance.

Item 12. Work permit

If required, check the appropriate box to indicate whether a copy of the work permit is attached. See AE Reg 190-16 for guidance.

Item 13. Type pass requested

Check the appropriate box. If an installation pass is desired, a temporary installation pass may be issued pending completion of a required background check. A temporary installation pass is valid for up to 90 days. The restrictions associated with each pass are different for each individual's access requirements.

Item 19. Installations for which access is required

Enter the level of access required. Depending on the person category, access may be restricted per AE Reg 190-16. Access should be limited to the least amount required. Examples include Taylor Barracks; 293d BSB (Mannheim); 26th ASG-wide; USAREUR-wide (Germany only).

The following levels of USAREUR-wide access are available:

- USAREUR/USAFE-wide
- USAREUR-wide
- USAREUR/USAFE (Germany only)
- USAREUR (Germany only)

NOTE: If liberal access is required, the sponsoring organization and the IACS registrar must take steps to ensure the proper selection from the above is made. For example, a contractor who operates exclusively within Germany should never be given USAREUR/USAFE-wide access.

Item 19. Installations for which access is required (continued)

If any level of USAREUR-wide access is requested above, the sponsoring official must include a written justification in item 27. The written justification must demonstrate why the applicant requires the level of access in the performance of duties. NATO Member and Department of State and American Embassy person categories are defaulted to USAREUR/USAFE-wide access; no justification is required.

Item 20. Limitations/time/day access is required

Enter "24/7" if access is required all the time; otherwise state the specific days of the week and times. IACOs may require justification for liberal access (such as 24/7), so sponsoring organizations should be prepared to justify this entry.

Item 21. FPCON restriction

Enter the FPCON restriction. The IACS will establish a default FPCON according to AE Reg 190-16. Sponsoring officials may request a reduction or a one-FPCON increase.

- Delta
- Charlie
- Bravo
- Alpha

Item 22. Pass expiration date

Enter the desired installation pass expiration date. This field will be validated by the IACO. Justification for this date must be provided. A temporary installation pass is valid for up to 90 days. The expiration date of an installation pass depends on the limitations of the person category (item 7) selected as well as the expiration date of the supporting document (for example, passport) that was used to obtain the installation pass. The expiration date will be whichever date is earlier.

Item 23. Sign-in privileges

Check the appropriate box to indicate whether sign-in privileges are required. If sign-in privileges are requested, the sponsoring official must include a written justification in item 28. The written justification must demonstrate why the applicant requires sign-in privileges in the performance of duties. NATO Member and Department of State and American Embassy person categories are defaulted to sign-in privileges authorized; no justification is required.

Item 24. Privately owned vehicle (POV) registration information

- a. State the license plate number exactly as it appears.
- b. State the country the license plate was issued for.
- c. State the make of the vehicle (for example, Opel, Saab, BMW).
- d. State the model of the vehicle (for example, 325i, Astra, 190E, S60).
- e. State the year of the vehicle (YYYY).
- f. State the body type of the vehicle (for example, 2-door sedan, bus).
- g. State the color of the vehicle.

Item 25. Company name and telephone number

This item is only applicable for applicants in the Contractor (living in host nation) person category. If applicable, enter the name and telephone number of the company.

Item 26. Verification by sponsoring official authority

State the name, title, organization, and telephone number of the sponsoring official. The BSB IACO must have a copy of the designation of sponsoring officials memorandum from your organization identifying who is authorized to sign installation pass applications.

Item 27. To be completed by registrar.

Item 28. Installations for which access is required

Enter the written justification that demonstrates why the applicant requires the level of access in the performance of duties.

Item 29. Sign-in privileges

Enter the written justification that demonstrates why the applicant requires sign-in privileges in the performance of duties.

ANHANG D

UMRECHNUNGSTABELLE FÜR KÖRPERGRÖSSE UND KÖRPERGEWICHT

**Umrechnung - Gewicht
(2,2045 Pfund = 1 kg)**

Gewicht in kg	Entsprechung in Pfund
35	77
37	82
39	86
41	90
43	95
45	99
47	104
49	108
51	112
53	117
55	121
57	126
59	130
61	134
63	139
65	143
67	148
69	152
71	157
73	161
75	165
77	170
79	174
81	179
83	183
85	187
87	192
89	196
91	201
93	205
95	209
97	214
99	218
101	223
103	227
105	231
107	236
109	240
111	245
113	249
115	254
117	258
119	262
121	267
123	271
125	276
127	280
129	284
131	289
133	293
135	298
137	302

**Umrechnung - Körpergröße
(0,39370 Inches = 1 cm)**

Größe in cm	Größe in Feet und Inches	Größe in Inches
122	4 feet 0 inches	48
124	4 feet 1 inches	49
127	4 feet 2 inches	50
130	4 feet 3 inches	51
132	4 feet 4 inches	52
135	4 feet 5 inches	53
137	4 feet 6 inches	54
140	4 feet 7 inches	55
142	4 feet 8 inches	56
145	4 feet 9 inches	57
147	4 feet 10 inches	58
150	4 feet 11 inches	59
152	5 feet 0 inches	60
155	5 feet 1 inches	61
157	5 feet 2 inches	62
160	5 feet 3 inches	63
163	5 feet 4 inches	64
165	5 feet 5 inches	65
168	5 feet 6 inches	66
170	5 feet 7 inches	67
173	5 feet 8 inches	68
175	5 feet 9 inches	69
178	5 feet 10 inches	70
180	5 feet 11 inches	71
183	6 feet 0 inches	72
185	6 feet 1 inches	73
188	6 feet 2 inches	74
191	6 feet 3 inches	75
193	6 feet 4 inches	76
196	6 feet 5 inches	77
198	6 feet 6 inches	78
201	6 feet 7 inches	79
203	6 feet 8 inches	80
206	6 feet 9 inches	81
208	6 feet 10 inches	82
211	6 feet 11 inches	83

ANHANG E
ANERKENNUNG DER PFLICHTEN EINES AUSWEISINHABERS (MUSTERSCHREIBEN)

MEMORANDUM FOR RECORD	Date	
SUBJECT: Acknowledgement of Installation-Pass-Holder Responsibilities		
1. Reference AE Regulation 190-16, Installation-Access Control, 18 January 2005.		
2. As a USAREUR/USAFE Installation Pass holder, I acknowledge the following:		
a. All persons, their personal property, U.S. Government property, and vehicles may be searched on entry, while within the confines of, or when leaving U.S. Forces installations. Persons attempting to gain entry who refuse to identify themselves, provide digitized fingerprint minutia data (DFMD), or consent to search will be denied access.		
b. If I am authorized sign-in privileges, I understand that at no time will I have more than four persons and their vehicles signed in. I understand that by signing for another person to enter a U.S. Forces installation, I am agreeing to monitor that person's actions at all times, and I accept full responsibility for that person's conduct. I will ensure that the signed-in person complies with U.S. Forces and local policy.		
c. Installation Passes are U.S. Government property. Any access-control person may confiscate an Installation Pass that has expired, is being used fraudulently, is being presented by a person other than the person to whom it was issued, or is obviously altered, damaged, or mutilated.		
d. I must surrender my pass when—		
(1) It is replaced (except when lost or stolen).		
(2) I no longer require access.		
(3) My sponsor-status changes.		
(4) I resign or retire, am terminated, or am no longer officially sponsored.		
e. If I lose my Installation Pass or if it is stolen, I must immediately notify either the MP or installation access-control office that issued the pass. Failure to do so is grounds for denying a replacement pass.		
f. Violations of U.S. Forces security policy may be grounds for denying access to U.S. Forces installations and lead to confiscation of installation-access documents.		
3. I acknowledge by my signature that I have read and understand the policy, requirements, and responsibilities above.		
_____	_____	_____
(Print) Last, First, MI	Signature	Date

GLOSSAR

TEIL I ABKÜRZUNGEN

<i>Ist PERSCOM</i>	<i>1st Personnel Command</i>
<i>AAFES-Eur</i>	<i>Army and Air Force Exchange Service, Europe</i>
<i>ACP</i>	<i>Acces-Control Point</i>
<i>AOR</i>	<i>Area of Responsibility</i>
<i>ASG</i>	<i>Area Support Group</i>
<i>AST</i>	<i>Area Support Team</i>
<i>BSB</i>	<i>Base Support Battalion</i>
<i>CAC</i>	<i>Common Access Card</i>
<i>COR</i>	<i>Contracting Officer's Representative</i>
<i>CPAC</i>	<i>Civilian Personnel Advisory Center</i>
<i>CPF</i>	<i>Central Processing Facility</i>
<i>DCII</i>	<i>Defense Clearance and Investigation Index</i>
<i>DOD</i>	<i>Department of Defense</i>
<i>EU</i>	<i>Europäische Union</i>
<i>FNS</i>	<i>Foreign National Screening</i>
<i>FPCON</i>	<i>Force Protection Condition</i>
<i>G2</i>	<i>Deputy Chief of Staff, G2, USAREUR</i>
<i>IACO</i>	<i>Installation Access Control Office</i>
<i>IACS</i>	<i>Installation Access Control System</i>
<i>ID</i>	<i>Identification</i>
<i>IMA-E</i>	<i>United States Army Installation Management Agency, Europe Region Office</i>
<i>JA</i>	<i>Judge Advocate, USAREUR</i>
<i>MIPR</i>	<i>Military Interdepartmental Purchase Order</i>
<i>NATO</i>	<i>North Atlantic Treaty Organization</i>
<i>PMO</i>	<i>Provost Marshal Office</i>
<i>PR&C</i>	<i>Purchase Request and Commitment</i>
<i>SCOR</i>	<i>Site Contracting Officer's Representative</i>
<i>TM</i>	<i>Technical Manual</i>
<i>U.S.</i>	<i>United States</i>
<i>USAFE</i>	<i>United States Air Forces in Europe</i>
<i>USAREUR</i>	<i>United States Army, Europe</i>

TEIL II BEGRIFFE

Antrag

Kasernenausweise werden mit Formblatt *AE Form 190-16A* beantragt.

Antragsteller

Jemand, der einen Antrag auf Ausstellung eines Kasernenausweises stellt.

Beantragende Person

Ein Inhaber einer *DOD ID-Card*, der für einen Dritten einen Kasernenausweis beantragt, aber nicht dazu berechtigt ist, die Aufgaben einer *Sponsoring Organization* wahrzunehmen. Beantragende Personen treten nur in der Kategorie „Hausangestellte“ (Abs. 16) und in den beiden „Besucher-„Kategorien (Abs. 23 und 24) auf.

Eintragung in Besucherlisten

Diese Berechtigung wird Angehörigen bestimmter Personengruppen gewährt. Damit wird Personen gestattet, Besucher nach deren Eintragung in Besucherlisten in den Einrichtungen zu begleiten.

Foreign National Screening Program

Dieses Programm wird vom *USAREUR G2* durchgeführt und dient der Überprüfung nicht-amerikanischer Staatsbürger.

In loco parentis

An Eltern statt

Installation Access Control Office

Eine in der Regel auf *Base Support Battalion/Area Support Team*- Ebene eingerichtete und vom *Provost Marshal, USAREUR* genehmigte Stelle, deren Aufgabe es ist, Mitarbeiter im *Installation Access Control System* zu registrieren sowie Kasernenausweise zu erstellen und auszustellen.

Installation Access Control System

Computergestütztes System, mit dessen Hilfe das *USAREUR Installation Access Control Program* (Programm zur Zugangskontrolle) durchgeführt wird.

Kontrollierte Einrichtungen

Alle Einrichtungen der US-Streitkräfte, bei denen der Zugang durch Wachposten kontrolliert wird.

Logischer Zugang

Unter „logischem“ Zugang versteht man den Zugang/Zugriff zu elektronischen Zugangskontrollsystemen (Computer) ohne Berechtigung des physischen Zugangs zu Einrichtungen.

Mitarbeiter verpflichteter Privatfirmen

Im Rahmen eines mit dem US-Verteidigungsministerium abgeschlossenen Vertrags tätige Personen. Darin eingeschlossen sind *Primary Contractor* (Mitarbeiter verpflichteter Privatfirmen, die direkt dem Inhaber einer *DOD ID-Card* oder einem vollzeitbeschäftigten ortsansässigen Arbeitnehmer unterstellt sind), vom *Primary Contractor* verpflichtete Personen sowie Einzelpersonen, die im Rahmen eines ausschließlich mit ihnen abgeschlossenen Vertrags, tätig sind.

Personengruppe

Bei der Erfassung im *Installation Access Control System* werden Personen einer von 18 „Personengruppen“ zugeordnet. Maßgebend dafür ist das Verhältnis, in welchem die Personen zu *USAREUR* stehen. Für jede Personengruppe gelten aufgrund des Sicherheitsrisikos, das die Gruppe darstellt, spezielle Voraussetzungen für die Registrierung im *IACS* und Beschränkungen im Hinblick auf die Zugangsberechtigung. Inhaber von *DOD ID-Card* werden einer Gruppe zugeordnet, während bei den Inhabern von Kasernenausweisen unter 17 Personengruppen unterschieden wird.

Registrator

Ein Mitarbeiter, der bevollmächtigt ist, Personen im *Installation Access Control System* zu registrieren und Kasernenausweise auszustellen. Registratoren arbeiten in der Regel im *Installation Access Control Office*.

Registrierungsliste

Eine der vier Möglichkeiten, aufgrund derer Zugang zu kontrollierten Einrichtungen von *USAREUR* gewährt werden kann. Eine Registrierungsliste ist eine genehmigte Liste, auf der alle Personen aufgeführt sind, die ohne Begleitung Zugang zu einer *USAREUR*-Einrichtung haben.

Sponsoring Official

Ein Mitarbeiter, der im Auftrag der *Sponsoring Organization* deren Aufgaben wahrnimmt. *Sponsoring Officials* sind schriftlich zu bestellen.

Sponsoring Organization

Mit *Sponsoring Organization* wird diejenige Organisation bezeichnet, die aufgrund ihres Verhältnisses zum Antragsteller auf einen Kasernenausweis bestimmte Aufgaben im Hinblick auf die Ausweisausstellung wahrnimmt. Welche Organisation als *Sponsoring Organization* zu fungieren hat, ist für jede Personengruppe angegeben. *Sponsoring Organizations* prüfen, ob die Erfordernis, dass der Antragsteller Zugang zu *USAREUR*-Einrichtungen benötigt, rechtmäßig ist. Für jeden, der einen Kasernenausweis beantragt bzw. besitzt, trägt eine *Sponsoring Organization* die Verantwortung und hat im Rahmen des *USAREUR Installation Access Control Program* wichtige Aufgaben wahrzunehmen.

Unbrauchbarer Kasernenausweis oder unbrauchbare *DOD ID-Card*

Unbrauchbar bezieht sich auf den Zustand eines Ausweises bzw. auf an ihm vorgenommene Änderungen, aufgrund derer es dem Wachposten unmöglich ist, den Ausweis zu überprüfen und sicherzustellen, daß die den Ausweis vorlegende Person auch Inhaber des Ausweises ist bzw. aufgrund derer berechnete Zweifel an der Authentizität des Ausweises bestehen. Ausweise mit kleinen Knicken, sich lösendem Sicherheitsüberzug, verbläbter Schrift oder anderen Mängeln, die es dem Wachposten erlauben, die den Ausweis vorlegende Person als Ausweisinhaber zu identifizieren, gelten nicht als unbrauchbar.

DATENSCHUTZERKLÄRUNG

Die Regierung der Vereinigten Staaten von Amerika sieht sich in besonderer Weise dem Schutz der Privatsphäre des Individuums verpflichtet. Als Teil der Executive achtet das US-Verteidigungsministerium auf den Schutz persönlicher Daten, die im Rahmen dienstlicher Belange von Mitarbeitern, Vertragsnehmern und dritten Personen erhoben werden müssen. Dabei wenden die Dienststellen des Verteidigungsministeriums im Ausland das jeweils einschlägige nationale Datenschutzrecht an.

Im Hinblick auf die Bedrohung durch den internationalen Terrorismus sind die Dienststellen der US Streitkräfte bemüht den grösstmöglichen Schutz von Personal, Gerätschaften und Liegenschaften vor Anschlägen sicherzustellen. Hierzu ist es erforderlich, den Zugang zu den Liegenschaften zu beschränken und sicherzustellen dass nur berechtigte Personen Zugang erhalten. Diesem Zweck dient die Einführung eines mit biometrischen Daten (digitalisiertes Lichtbild und zwei Fingerabdrücke) ausgestatteten Ausweises, der Installation Access System Control Card, der eine schnelle und sichere Personenidentitätsfeststellung ermöglicht.

Ihre mit dem Antragsformular 190-16A zu den Nummern 4-10,13-25 erhobenen persönlichen Daten werden in eine regionale Datenbank des Installation Access Systems (IACS) aufgenommen und gespeichert. Dies gilt auch für die digitalisierten Fingerabdrücke und das Lichtbild. Für die Datenbank ist das Office of the Provost Marshall verantwortlich.

Die Daten werden ausschliesslich zur Identitätsüberprüfung im Zusammenhang mit dem Zugang zu und dem Aufenthalt in Einrichtungen der US Streitkräfte verwendet. Sie werden durch Zugangskontrollsysteme entsprechend dem jeweiligen Stand der Technik gegen unberechtigten Zugriff geschützt und sind nur dem mit der Aufgabe des Liegenschaftsschutzes betrauten Personenkreis zugänglich. Durch die Lesegeräte wird über einen automatischen Abgleich der auf dem Ausweis verschlüsselt enthaltenen Daten mit der Datenbank die Echtheit des Ausweises überprüft.

Eine Übermittlung der Daten an Stellen ausserhalb der Bundesrepublik Deutschland erfolgt nicht. Mit dem Liegenschaftsschutz betraute Dienststellen des U.S.-Verteidigungsministeriums in Europa haben zu Zwecken der Personenzugangskontrolle Zugriff auf die gespeicherten Daten, wenn die betroffene Person eine in Europa ausgestellte Installation Access Control Card vorlegt. Eine Übermittlung von Daten an Dienststellen der Bundesrepublik Deutschland erfolgt nur soweit dies nach den rechtlichen Bestimmungen des Bundesdatenschutz-gesetzes zulässig ist.

Bei einem Ausscheiden aus dem Dienst bei den US Streitkräften bzw. bei Wegfall der Notwendigkeit, im Rahmen dienstlicher oder vertraglicher Belange Liegenschaften der US Streitkräfte zu betreten, werden die gespeicherten Daten in ein gesichertes Datenarchiv transferiert und dort nach einem Zeitraum von 5 Jahren vollends gelöscht.

Andere als die mit der Antragsstellung angeforderten persönlichen Daten werden nicht erhoben. Der Antragsteller ist befugt beim zuständigen IACS-Office unentgeltlich Auskunft über die über ihn gespeicherten Daten und gegebenenfalls deren Korrektur zu verlangen.

Die Hauptbetriebsvertretung der bei den US-Streitkräften beschäftigten Ortskräfte hat der Erhebung, Speicherung und Verwendung der persönlichen Daten im Zusammenhang mit der Einführung des neuen Liegenschaftszugangkontrollsystems zugestimmt.

Von der vorstehenden Datenschutzerklärung habe ich Kenntnis genommen. Mir ist bekannt, dass eine Verweigerung der Einwilligung zur Verweigerung des Zugangs zu den Liegenschaften führen kann. Dies kann – mit weiteren Folgen – dazu führen, dass ich meinen vertraglichen Verpflichtungen nicht nachkommen kann.

Ich stimme der Speicherung meiner Daten in der IACS Datenbank zu.

(Ort, Datum)

(Unterschrift)

Translation

PRIVACY ACT STATEMENT

The Government of the United States of America considers itself especially obligated to protect individual privacy. The Department of Defense (DoD), as part of the executive branch, attaches great importance to the protection of personal data, which have to be collected from employees, contractors and third parties within the scope of official requirements. DoD agencies abroad are complying also with the respective national data protection laws.

In view of the threat posed by international terrorism, US Forces agencies are attempting to provide maximum protection against terrorist attacks for personnel, equipment and accommodations. In order to achieve this, it is necessary to limit access to the accommodations and to ensure that authorized persons only have access. For this purpose, an ID-Card containing biometric data (digitized photo and two finger prints) - the Installation Access Control System Card was introduced, making a fast and certain personnel identification possible.

Your personal data collected on Application Form 190-16A under Item 4 to 10 and 13 to 25 will be stored in a regional data base of the Installation Access Control System (IACS). This also applies to the digitized finger prints and the photo. The Office of the Provost Marshal is responsible for the data base.

The data will be used exclusively for individual identification in connection with access to and presence on US Forces installations. The data will be protected against unauthorized access by state of the art access control systems and will be accessible only for the category of personnel responsible for installation protection. By applying the screening device in order to compare the encrypted data on the ID-cards to the data in the data base, the authenticity of the ID-card will be verified.

The data will not be transferred to agencies outside of the Federal Republic of Germany. This does not apply to the transfer of data to activities of the US Forces located in Europe for identification purposes in connection with granting access to installations of the US Forces in those countries. The recipient is not authorized to transfer the data any further. Data will be transferred to agencies of the Federal Republic of Germany only if permissible under the statutory provisions of the Federal Republic of Germany.

In the case of termination of employment with the US Forces, respectively, if access to the installations within the scope of official or contractual purposes is no longer required, the personal data will be transferred to a secure data archive and will be deleted entirely after 5 years.

Other data than those requested upon application will not be collected. The applicant is authorized to demand free-of-charge information from the responsible IACS Office concerning the data stored about him/her and, if applicable, may demand correction.

The Head Works Council of the Local Nation employees of the US Forces has consented to the collection, storage and utilization of personal data in connection with the introduction of the new Installation Access Control System.

I have taken notice of the above Privacy Act Statement. I am aware that my refusal to consent may result in denial of access to the installations. This may result – with further consequences - in my inability to comply with my obligations.

I consent to the storage of my data in the IACS data base.

(location, date)

(signature)